Privacy and Civil Liberties Implementation Workbook

For Federal Agencies

Version 1.1

Page is intentionally left blank.

Privacy and Civil Liberties Implementation Workbook

For Federal Agencies

Version 1.1

For more information and latest Workbook updates, go to

www.ise.gov/pages/privacy-implementing.html

Page is intentionally left blank.

Table of Contents

Page is intentionally left blank.

Workbook Introduction

The Privacy and Civil Liberties Implementation Workbook (the Workbook) is an additional tool designed to complement the Information Sharing Environment (ISE) Privacy and Civil Liberties Implementation Guide (the Guide). While the Guide provides an overall process for agencies to follow in implementing the ISE Privacy Guidelines, the Workbook provides practical, step-by-step assistance to individuals within federal agencies[1] who will be tasked with implementing the Guidelines. It is also intended to serve as a "one-stop shop" of key guidance documents and tools for ISE Privacy Officials and privacy and civil liberties officers, providing important references in one convenient location.

The Workbook covers the implementation process from start to finish. However, much like the Guide, it is flexible in its application. It can be used in any order—in whole or in part—depending on where an agency is in its implementation of the Guidelines.

After completing the Workbook, an agency should have a written, complete ISE privacy protection policy. The Workbook will also help identify ongoing compliance and implementation issues for an agency to consider.

The Workbook is divided into five sections: Get Your Bearings; Identify What Your Agency Is Doing; Assemble Your Toolkit; Identify—Assess—Protect x 2; and Ongoing Implementation and Compliance. It also includes key guidance documents and tools, which are conveniently gathered together for ease of reference:

Before starting, review the entire Workbook to become familiar with its organization and structure, and determine where your agency should begin. The review should help map out the steps, tasks, and decisions that still need to be undertaken, as well as the available resources which might be used to assist your agency's implementation efforts. Agencies will most likely be at different starting points and stages/steps of implementation. Some agencies may be at the beginning, while other agencies may

[1] All references herein to federal agencies or federal departments and agencies are limited to federal executive branch departments and agencies.

have already completed many of the tasks. Agencies should not feel the need to repeat or duplicate any activity that may satisfy a task or step.

Below is an overview of the resources and tools associated with the steps, tasks, and decision points in each section.

Section 1—Get Your Bearings. This section assists agency officials and personnel in understanding the ISE, the ISE Privacy Guidelines, and the requirement to implement them in order to enhance privacy and civil liberties protections in the sharing of terrorism-related information. One training presentation and two short documents are available to assist an agency in undertaking this section.

- ISE 101—This presentation provides a basic overview of the ISE, a discussion of the ISE Privacy Guidelines requirements, and the requirement to implement the Guidelines. This presentation could be part of a briefing for key stakeholders, including senior leadership, system administrators, operational personnel, and privacy/civil rights/civil liberties officials. Currently under development, it will contain a PowerPoint presentation and speaker notes.
- *How the ISE Privacy Guidelines Help Senior Leadership*—This document could be used as part of a briefing on the ISE and the Privacy Guidelines when an in-depth discussion on the topic is not needed. In addition, the companion piece for federal employees could also be used. Both documents are already posted on www.ise.gov.

Section 2—Identify What Your Agency Is Doing. This section begins the process of identifying what a federal agency is currently doing within the ISE and identifying key personnel and program offices that may manage terrorism-related information. In addition, this section identifies several key decision points that an agency will need to consider before it moves forward. The determinations an agency makes will help map out how an agency proceeds.

Section 3—Assemble Your Toolkit. This section identifies tools and resources that will be needed in Section 4. These tools include:

ISE Privacy Guidelines
ISE Privacy and Civil Liberties Implementation Manual, including the Implementation Guide and the Key Issues Guidance

Section 4—Identify—Assess—Protect x 2. This section walks the user through the methodology outlined in the Implementation Guide. It provides practical additional information or suggestions and identifies where help is available, either through additional tools or via the information@AskPGC.org feature. As previously discussed in the Guide, STAGE I focuses on privacy/civil liberties officials and legal advisors, while STAGE II is oriented toward operational groups applying the ISE privacy policy to systems and sharing arrangements in the ISE.

STAGE I tools
2006 Interagency Compilation of Federal Privacy and Civil Liberties Policies That Impact Information Sharing
Policy Development Tool
ISE Privacy Policy Outline
Chart of Publicly Available Federal Privacy Policies

STAGE II tools

Steps for Assessing Federal Agency Systems of Records (Definitional Scope for the ISE Privacy Guidelines)

Section 5—Ongoing Implementation and Compliance. The final section addresses the continuing cycle of training on ISE issues and the ISE Privacy Guidelines, reviewing policies, applying the Guidelines to new systems, and tracking performance measures.

Appendices. Key guidance and tools have been included in the appendices so that important references are easily accessible.

Appendix A—ISE Privacy Guidelines: Issued in December 2006, the Guidelines provide the framework for enabling information sharing while protecting privacy and other legal rights.

Appendix B—2006 Interagency Compilation of Federal Privacy and Civil Liberties Policies That Impact Information Sharing: This compilation is the result of the initial data call for privacy and civil liberties laws, Executive Orders, policies, and procedures. This should not be viewed as an exhaustive list but as a starting point for agencies.

Appendix C—Policy Development Tool: This tool is designed to assist agencies conducting a review of existing policies and procedures compared to the ISE Privacy Guidelines requirements and to identify any gaps in policy coverage.

Appendix D—Key Issues Guidance: Developed and approved by the Privacy Guidelines Committee, this document offers guidance in interpreting certain ISE Privacy Guidelines requirements and outlines possible methods to assist agencies in implementing those requirements.

Appendix E—ISE Privacy Policy Outline: This tool is designed to assist agencies in developing their ISE privacy protection policy.

Appendix F—Steps for Assessing Federal Agency Systems of Records: Initially approved by the Privacy Guidelines Committee in May 2007, this definitional scope document provides federal agencies with a workable approach for applying the ISE Privacy Guidelines to systems of records that contain information within the scope of the ISE.

Appendix G—Chart of Publicly Available Federal Privacy Policies: This tool is a reference to existing published federal agency privacy policies.

Appendix H—ISE Privacy Guidelines Definitions: A list of key definitions for the Information Sharing Environment Privacy Guidelines.

If at any point during this process a privacy official has questions or needs assistance, he or she should send an e-mail to information@AskPGC.org or call (202) 429-2712.

Section 1. Get Your Bearings

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION

☐	**Task—Understand the Information Sharing Environment (ISE) definition/concept.**	• The ISE is an approach.
		• It is the policies, process/protocols, and technology that enable the sharing of terrorism-related information among federal, state, local, tribal, and private sector entities, as well as foreign partners, by federal agencies.
		• If you have questions,
		  ○ See www.ise.gov.
		  ○ Consult the "ISE Privacy Guidelines Frequently Asked Questions" (FAQs).
		  ○ Consult your agency's representative on the Information Sharing Council[2] (ISC).
		• Situational awareness:
		  ○ Information is being shared for counterterrorism and law enforcement purposes.
		  ○ Policies, process/protocols, and technology enable sharing.
		  ○ Do not wait for "a place or information system" to be built.
		HELP AVAILABLE
		• All resources are on www.ise.gov.
		  ○ ISE 101 presentation
		  ○ ISE Implementation Plan
		  ○ *National Strategy for Information Sharing*

☐	**Task—Understand the requirements of the ISE Privacy Guidelines.**	• Issued in December 2006. • Apply to existing and new or planned terrorism-related information sharing systems and sharing arrangements by federal agencies. **HELP AVAILABLE** • ISE Privacy Guidelines, **Appendix A** • "ISE Privacy Guidelines FAQs" • *How the ISE Privacy Guidelines Help Senior Leadership* • *How the ISE Privacy Guidelines Help Federal Employees*

[2] Agencies of the ISC can be found at www.ise.gov/pages/isc.html.

TASKS/DECISION POINTS	STILL TO DO
Task—Understand the ISE definition/concept.	
Task—Understand the requirements of the ISE Privacy Guidelines.	

Section 2.
Identify What Your Agency Is Doing

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**Task—Identify who in your agency is key to implementing the ISE Privacy Guidelines.**	• Representatives assigned to ISE bodies. • Program offices charged with sharing terrorism-related information. • Operators, analysts, managers, and others who deal with terrorism information. • Agency counsel who deal with civil liberties or civil rights issues raised by agency action. • If your agency has a compliance or complaint handling unit, consider a representative who might be able to identify any civil liberties/civil rights issues raised or complaints made by members of the public.
☐	**Task—Identify your agency's terrorism-related information sharing activities.**	• Existing and planned. • However labeled ("ISE" or otherwise). Examples: MOUs Routine uses Bulk sharing Individualized requests
☐	**Task—Identify steps your agency already has taken toward establishing and implementing a privacy protection policy.**	• Has an agency privacy protection policy been issued? • Does it extend to the ISE?

TASKS/DECISION POINTS	STILL TO DO
Task—Identify who in your agency is key to implementing the ISE Privacy Guidelines.	
Task—Identify your agency's terrorism-related information sharing activities.	
Task—Identify steps your agency already has taken toward establishing and implementing a privacy protection policy.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION

☐	**Decision Point—Determine whether your agency will have a single ISE privacy policy for the entire organization or whether each component will develop its own.**	Agencies have several options:
		• Issue a global agency policy that is department-/agency-wide.
		• Issue a directive ordering all components to develop ISE-compliant policies specific to their organizations.
		  o An agency may have individual policies for various components.
		  ▪ Agencies may have a policy for components that do not significantly engage in ISE work, while directing other components that do engage in ISE work, to develop their own privacy policies.

☐	**Decision Point—Determine whether your agency will involve nongovernmental organizations, privacy advocates, an advisory board, or an internal working group in the policy development process.**	While not required by the ISE Privacy Guidelines, agencies may choose to include others in their development or review process. It is useful to know this at the outset so appropriate interaction may be obtained at each stage of policy development. Agencies should be aware that consultation with elements outside the federal government may require compliance with the Federal Advisory Committee Act (FACA).
☐	**Decision Point—Determine how your agency will address public awareness of your ISE privacy protection policy.**	Section 10 of the ISE Privacy Guidelines states: "Each agency shall take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines." Agencies may satisfy this requirement in any manner. Some may choose to post the policy on their Web site. Others may make it available upon request. Keep in mind that whatever mechanism is chosen may affect the format of the policy.

TASKS/DECISION POINTS	STILL TO DO
Decision Point—Determine whether your agency will have a single ISE privacy policy for the entire organization or whether each component will develop its own.	
Decision Point—Determine whether your agency will involve nongovernmental organizations, privacy advocates, an advisory board, or an internal working group in the policy development process.	
Decision Point—Determine how your agency will address public awareness of your ISE privacy protection policy.	

Section 3. Assemble Your Toolkit

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**Task—Development Process**	
☐	1) Review the Manual.	See www.ise.gov and review the Privacy and Civil Liberties Implementation Manual, particularly the: • Implementation Guide • Key Issues Guidance Consult the "ISE Privacy Guidelines FAQs"
		HELP AVAILABLE • Need Help? E-mail your questions to information@AskPGC.org.
☐	2) Determine whether your agency has already undertaken activities that need to be completed as part of the Identify—Access—Protect methodology. • For example, has your agency already identified terrorism-related information systems or sharing arrangements? Has your agency conducted a rules assessment?	Gather relevant documents to avoid duplicating steps already completed. The Implementation Guide suggests a methodology (Identify—Assess—Protect) for assessing current privacy protection efforts and developing a written ISE privacy protection policy. The Guide is located at www.ise.gov.

TASKS/DECISION POINTS	STILL TO DO
Task—Development Process	
1) Review the Manual.	
2) Determine whether your agency has already undertaken activities that need to be completed as part of the Identify—Access—Protect methodology.	

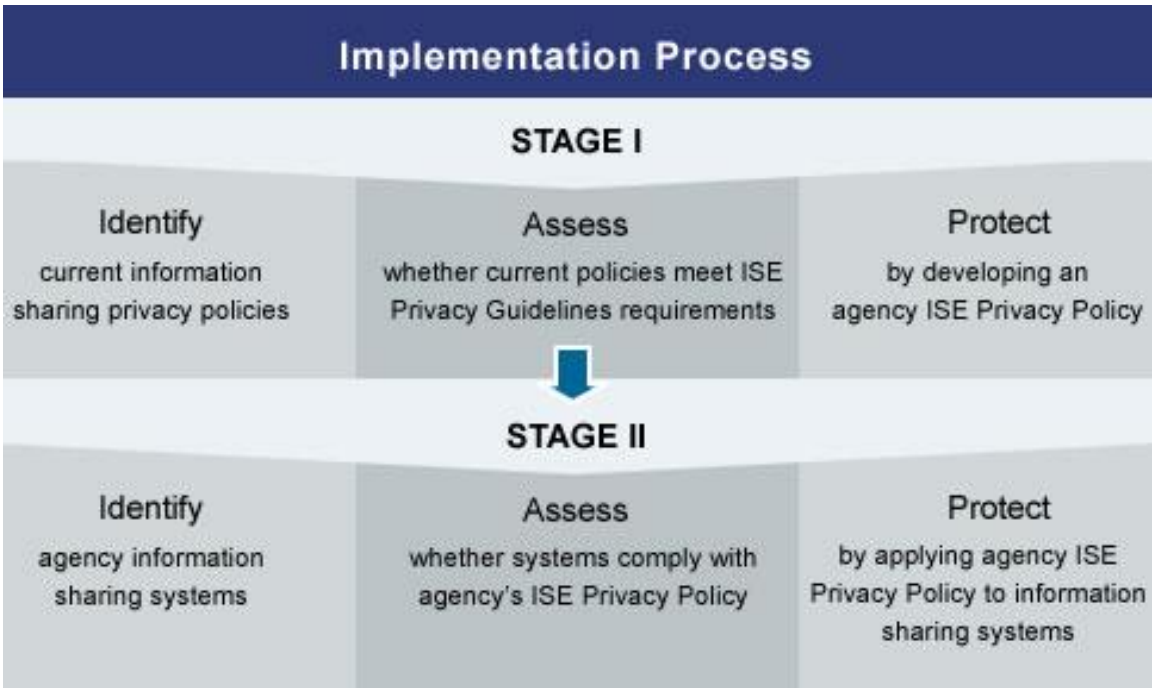
COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**Task—Planning for Agency Approval/Adoption of ISE Privacy Protection Policy**	
☐	1) Identify your agency process for approving/adopting a written ISE privacy protection policy.	This process may depend on how your agency decides to issue the policy; i.e., whether it is a new issuance (new content) versus a compilation of (incorporation by reference to) existing policies or a combination of approaches.
☐	2) Identify preparations that can be made at this stage to help the approval/adoption process move smoothly.	Examples of preparatory activities: • Meet with appropriate senior leadership and key stakeholders to ensure they understand the ISE, the Privacy Guidelines, and the requirement to implement an ISE privacy protection policy. • Obtain agreement on scope of policy to be issued: agency-wide, component-specific. • Develop an implementation plan outlining the process for developing the policy, identifying key components/stakeholders involved, and establishing a timeline for completion.
☐	**Task—Determining Format of Policy**	
☐	1) Determine how your agency will produce the policy. • Will it be a new policy? • Will it cross-reference existing policies? • Both?	From a format perspective, an agency must consider how to most effectively present the policy—to its employees and to the public. The written ISE privacy protection policy may cross-reference existing policies, reproduce existing policies, articulate new or revised policy provisions that fill gaps, or combine any or all of these approaches. Agencies should not rely on ISE processes for policies that require vetting and approval by another agency or body; e.g., policies implementing the requirements of Executive Order 12333.

TASKS/DECISION POINTS	STILL TO DO
Task—Planning for Agency Approval/Adoption of ISE Privacy Protection Policy	
1) Identify your agency process for approving/adopting a written ISE privacy protection policy.	
2) Identify preparations that can be made at this stage to help the approval/adoption process move smoothly.	
Task—Determining Format of Policy	
1) Determine how your agency will produce the policy. • Will it be a new policy? • Will it cross-reference existing policies? • Both?	

Page is intentionally left blank.

Section 4. Identify—Assess—Protect x 2

As noted in the Workbook Introduction and in the Guide, steps underlying the Identify—Assess—Protect methodology can be accomplished sequentially or concurrently.



Step 1 of STAGE I and Step 1 of STAGE II can be performed simultaneously, or STAGE II, Step 1 could be performed before STAGE I, Step 1. While the order is less important than the individual steps, it is not possible to complete STAGE II, Steps 2 and 3 without having completed the initial steps in each stage.

An agency may have already completed these activities—possibly as part of a different effort. If that is the case, the agency does not need to repeat or duplicate activities that will suffice to satisfy a step. If a part of a step has already been accomplished, only the remaining part of the step needs to be completed. How an agency produces a written ISE privacy protection policy and implements the Information Sharing Environment (ISE) Privacy Guidelines depends on its unique environment and circumstances. As long as a policy is developed, it is not mandatory that agencies follow the framework provided here or in the Guide.

Note: With each new system or sharing arrangement, STAGE II will need to be repeated to ensure the agency's ISE privacy protection policy is met and the requirements incorporated into terrorism-related sharing activities. If new laws or Executive Orders are issued, STAGE I and STAGE II would need to be reviewed to ensure the new provisions are fully integrated into the policy and its application.

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**STAGE I—Step 1: Identify rules that apply to protected information shared in the ISE.**	
☐	1) Compile a list of existing federal laws, Executive Orders, policies, and procedures that apply to protected information that is or may be made available or accessed (shared) through the ISE.	Section 1(b) of the ISE Privacy Guidelines defines protected information as information about United States citizens or lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and federal laws of the United States. For the Intelligence Community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered by these Guidelines. **HELP AVAILABLE** An initial compilation of federal privacy and civil liberties policies that impact information sharing can be found (i) in the Manual (STAGE I, Step 1), (ii) under the Resources Tab on the ISE Web site, and (iii) in **Appendix B** to this Workbook.
☐	2) Determine whether your list includes all applicable government-wide, sector-specific, and agency-specific laws, Executive Orders, policies, and procedures.	Examples: Government-wide: • U.S. Constitution • Privacy Act • E-Government Act • Executive Order 12333 • OMB • FOIA • FISA Sector-specific: • Financial • Social Security • Transportation • Education • Health • Immigration • Trade/Commerce

TASKS/DECISION POINTS	STILL TO DO
STAGE I—Step 1: Identify rules that apply to protected information shared in the ISE.	
1) Compile a list of existing federal laws, Executive Orders, policies, and procedures that apply to protected information that is or may be made available or accessed (shared) through the ISE.	
2) Determine whether your list includes all applicable government-wide, sector-specific, and agency-specific laws, Executive Orders, policies, and procedures.	

<table>
<tr><th>COMPLETED</th><th>TASKS/DECISION POINTS</th><th>ADDITIONAL INFORMATION</th></tr>
<tr><td>☐</td><td>STAGE I—Step 1: Identify rules that apply to protected information shared in the ISE. (continued)</td><td></td></tr>
<tr><td rowspan="2">☐</td><td>3) Consider all stages of the information life cycle in compiling your agency's list of laws, Executive Orders, policies, and procedures applicable to protected information that is or may be made available or accessed (shared) through the ISE.
• Review agency policy to address complaints by individuals whose information is (or is not) in your system, including complaints involving civil liberties and civil rights.
o Information removed due to court expungement order or unlawful collection
o Erroneous information impairing ability to conduct business or travel
o Procedures for notice to originating agency of complaint</td><td>Areas to consider:
• Collection (Acquisition and Access)
• Retention
• Production
• Use
• Sharing
• Management
• Compliance/ Complaint
• Policy on expungement
• Redress procedures for individuals
HELP AVAILABLE
The above terms are defined in Guideline 2, located at www.ise.gov.</td></tr>
<tr><td colspan="2">This is the list of rules you will assess and compare to the ISE Privacy Guidelines to determine whether existing policies satisfy the ISE requirements or whether there are gaps to be filled.</td></tr>
</table>

TASKS/DECISION POINTS	STILL TO DO
STAGE I—Step 1: Identify rules that apply to protected information shared in the ISE. **(continued)**	
3) Consider all stages of the information life cycle in compiling your agency's list of laws, Executive Orders, policies, and procedures applicable to protected information that is or may be made available or accessed (shared) through the ISE.	
This is the list of rules you will assess and compare to the ISE Privacy Guidelines to determine whether existing policies satisfy the ISE requirements or whether there are gaps to be filled.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**STAGE I—Step 2: Assess existing protections and protections identified in the ISE Privacy Guidelines and identify gaps to be filled.**	
☐	1) To assess the adequacy of your agency's policies, compare the current policies with the requirements in the ISE Privacy Guidelines.	Consider asking the following questions as part of the assessment process. 1) What legal authorities are controlling or relevant? 2) What information may or may not be collected? 3) How can information be collected? 4) Who is eligible to receive information that is collected? a) Internally b) Externally 5) What are the agency's transparency policies? 6) What are the agency's redress policies? 7) What are the agency's accountability, enforcement, and training policies?
☐	2) Determine agency-wide information, privacy, and civil liberties policies, procedures, guidelines, and practices. • Your agency may need to work with component agencies to make this determination.	Does your agency apply the Fair Information Principles to Privacy Act records? • What about non-Privacy Act records? Consider reviewing the following items: • Minimum necessary shared • Limitations on redisclosure • Alerts as to reliability • Monitored disclosure • Retention practices • Security controls **HELP AVAILABLE** The Fair Information Principles are located at http://www.privacyrights.org/ar/fairinfo.htm.
☐	3) Determine whether your agency collects, stores, or uses commercial data. • Does your agency have policies about commercial data? • Does your agency need policies about commercial data?	Commercial data is information obtained from a commercial source. A source is considered to be commercial, even if it contains public government data, if your agency purchases that data from the source.

TASKS/DECISION POINTS	STILL TO DO
STAGE I—Step 2: Assess existing protections and protections identified in the ISE Privacy Guidelines and identify gaps to be filled.	
1) To assess the adequacy of your agency's policies, compare the current policies with the requirements in the ISE Privacy Guidelines.	
2) Determine agency-wide information, privacy, and civil liberties policies, procedures, guidelines, and practices.	
3) Determine whether your agency collects, stores, or uses commercial data.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
	STAGE I—Step 2: Assess existing protections and protections identified in the ISE Privacy Guidelines and identify gaps to be filled. (continued)	
☐	4) When comparing existing policies/ procedures to each of the ISE Privacy Guidelines requirements, your agency will find either: a) Existing privacy and civil liberties policies, procedures, or practices are sufficient to address the ISE Privacy Guidelines, or b) Gaps between current policy and the ISE Privacy Guidelines requirements.	**HELP AVAILABLE** See "Policy Development Tool" located in **Appendix C** of this Workbook. The tool is designed to assist agencies in comparing their existing policies/procedures against the ISE Privacy Guidelines and the Key Issues core elements. The "Key Issues Guidance," **Appendix D** of the Workbook, provides additional in-depth guidance on the following selected areas of the ISE Privacy Guidelines: • Redress • Notice Mechanisms • Data Quality • Data Security • Accountability, Enforcement, and Training The Key Issues Guidance can also be found in the Implementation Manual.
☐	5) Determine whether existing agency policy ensures that the agency seeks and retains only information it is permitted to seek and retain.	
☐	6) Has your agency identified any instances in which agency rules or policies significantly impede information sharing without being required to protect privacy? • What purpose is each restriction designed to serve? • Has the matter been raised with appropriate officials in accordance with the ISE Privacy Guidelines?	**HELP AVAILABLE** Consult Section 2c (ii) and (iii) of the ISE Privacy Guidelines for the process to be used to handle such issues.
	This is the comparison of existing policies or procedures and the ISE Privacy Guidelines requirements. It should identify where there are gaps in existing policy.	

TASKS/DECISION POINTS	STILL TO DO
STAGE I—Step 2: Assess existing protections and protections identified in the ISE Privacy Guidelines and identify gaps to be filled. (continued)	
4) When comparing existing policies/ procedures to each of the ISE Privacy Guidelines requirements, your agency will find either: a) Existing privacy and civil liberties policies, procedures, or practices are sufficient to address the ISE Privacy Guidelines, or b) Gaps between current policy and the ISE Privacy Guidelines requirements.	
5) Determine whether existing agency policy ensures that the agency seeks and retains only information it is permitted to seek and retain.	
6) Has your agency identified any instances in which interagency rules impede sharing without protecting privacy?	
This is the comparison of existing policies or procedures and the ISE Privacy Guidelines requirements. It should identify where there are gaps in existing policy.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**STAGE I—Step 3: Develop or document an agency ISE privacy protection policy.**	
☐	1) Determine whether your existing privacy protection policy extends to the sharing of protected information in the ISE.	
☐	2) Determine whether your agency's policies, protocols, and guidelines for information sharing do the following:	
	a) Define categories of information that may be shared.	
	b) Categorize entities or individuals with which/whom data may be shared, with appropriate restrictions for each.	For example—law enforcement agencies, intelligence agencies, private sector entities, and individuals who are the subjects of records.
	c) Identify information sources.	Information sharing sources include systems of records/databases.
	d) Identify information sharing methods.	For example—software applications or other media, such as telephone, e-mail, etc.
	e) Describe how sharing requests may be received.	See above.
	f) Describe what processing must be conducted prior to sharing.	For example—review, redaction, formatting.
	g) Describe information sharing-related protocols.	For example—encryption, deidentification/anonymization, documentation of disclosures, and auditing of releases.

TASKS/DECISION POINTS	STILL TO DO
STAGE I—Step 3: Develop or document an agency ISE privacy protection policy.	
1) Determine whether your existing privacy protection policy extends to the sharing of protected information in the ISE.	
2) Determine whether your agency's policies, protocols, and guidelines for information sharing do the following: a) Define categories of information that may be shared. b) Categorize entities or individuals with which/whom data may be shared, with appropriate restrictions for each. c) Identify information sources. d) Identify information sharing methods. e) Describe how sharing requests may be received. f) Describe what processing must be conducted prior to sharing. g) Describe information sharing-related protocols.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
	STAGE I—Step 3: Develop or document an agency ISE privacy protection policy. **(continued)**	
☐	3) Determine whether your agency information sharing policy is reflected in your information sharing arrangements. • Does the memorandum of understanding (MOU) or other agreement give effect to the ISE privacy protection policy?	Consider whether the agreement addresses the following elements in order to determine whether existing policy meets ISE Privacy Guidelines requirements. Does the agreement: a) Identify the parties to the agreement and their authorities (e.g., requester/ receiver and sender)? b) Require privacy and civil liberties protections (e.g., encryption, limited use, data retention, notice and consent of data subjects where applicable, minimum necessary disclosure, and redress, including corrective measures, such as notice to receiving agencies, for erroneous or defective classified or other protected materials)? c) Require security protections (e.g., firewalls, intrusion detection systems, physical security, training and awareness of staff, and personnel authorization and authentication)? d) Specify applicable laws and regulations (including exemptions therefrom)? e) Provide notice regarding the nature of the information, including limitations on reliability and accuracy? f) Provide for monitoring/auditing responsibilities of sender and receiver (e.g., methods, frequency, roles and responsibilities, and remediation of deficiencies)? g) Address any potential intersection with state law? • Sunshine laws • State freedom of information statutes

TASKS/DECISION POINTS	STILL TO DO
STAGE I—Step 3: Develop or document an agency ISE privacy protection policy. **(continued)**	
3) Determine whether your agency information sharing policy is reflected in your information sharing arrangements. • Does the MOU or other agreement give effect to the ISE privacy protection policy?	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
	STAGE I—Step 3: Develop or document an agency ISE privacy protection policy. **(continued)**	
☐	4) Determine whether your policy provides for: a) Inspection/audit of compliance with privacy and civil liberties policies and procedures. b) Prompt reporting of noncompliance with ISE privacy and civil liberties procedures. c) A mechanism to respond to incidents of noncompliance, including sanctions for individuals who negligently or willfully violate policy.	Example: 1) Review of computer matching and other data merges for implications under the Privacy Act; e.g., to identify needed systems of records notices and ensure application of data accuracy, completeness, and timeliness controls, as necessary. 2) Review of complaint processing procedures to ensure that: • Erroneous, deficient, or court-expunged information is being addressed properly. • The redress procedure is publicly known. • Civil rights/civil liberties (CR/CL) complaints are recognized and properly addressed. Examples of potential CR/CL complaints based on inaccurate or erroneous information include issues such as: • Individuals being denied benefits and privileges such as restrictions on travel. • Access to certain facilities. • Loss of a job. • Being stopped and searched based on incorrect information submitted to law enforcement agencies. 3) Review of policies and procedures to determine whether there are triggers for effective notice to receiving agencies when protected information is discovered to be inaccurate or deficient and may cause harm to the individual if not corrected or deleted.

TASKS/DECISION POINTS	STILL TO DO
STAGE I—Step 3: Develop or document an agency ISE privacy protection policy. **(continued)**	
4) Determine whether your policy provides for: a) Inspection/audit of compliance with privacy and civil liberties policies and procedures. b) Prompt reporting of noncompliance with ISE privacy and civil liberties procedures. c) A mechanism to respond to incidents of noncompliance, including sanctions for individuals who negligently or willfully violate policy.	.

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
	STAGE I—Step 3: Develop or document an agency ISE privacy protection policy. **(continued)**	
☐	5) If your agency has developed new policies to fill identified gaps, determine whether the new policies and/or procedures identify: a) The relevant federal laws, regulations, guidelines, interagency agreements or rules, policies, or other agency-specific directives driving each requirement, especially those restricting data sharing. b) The specific mandate action or end state. c) Any exemptions to each requirement that the agency may invoke or has invoked, if applicable. d) The specific officials and personnel affected by the requirement and those responsible for implementing and overseeing the requirement. e) The particular detailed procedures to be followed by each category of affected staff, including enforcement and assurance responsibilities.	See **Appendix E** of the Workbook; the ISE Privacy Policy Outline provides a format to assist an agency in formulating its ISE privacy protection policy.
	After completing this stage, you will have produced a written ISE privacy protection policy. Remember, an agency may complete this stage by ensuring that existing policies or procedures are sufficient to meet the requirements of the ISE Privacy Guidelines, by developing new policies to fill any gaps between existing policies and the requirements of the Guidelines, or by some combination of existing or new policies.	

TASKS/DECISION POINTS	STILL TO DO
STAGE I—Step 3: Develop or document an agency ISE privacy protection policy. **(continued)**	
5) If your agency has developed new policies to fill identified gaps, determine whether the new policies and/or procedures identify: a) The relevant federal laws, regulations, guidelines, interagency agreements or rules, policies, or other agency-specific directives driving each requirement, especially those restricting data sharing. b) The specific mandate action or end state. c) Any exemptions to each requirement that the agency may invoke or has invoked, if applicable. d) The specific officials and personnel affected by the requirement and those responsible for implementing and overseeing the requirement. e) The particular detailed procedures to be followed by each category of affected staff, including enforcement and assurance responsibilities.	
After completing this stage, you will have produced a written ISE privacy protection policy. Remember, an agency may complete this stage by ensuring that existing policies or procedures are sufficient to meet the requirements of the ISE Privacy Guidelines, by developing new policies to fill any gaps between existing policies and the requirements of the Guidelines, or by some combination of existing or new policies.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**STAGE II—Step 1: Identify systems and sharing arrangements in the ISE.**	
☐	1) Determine whether your agency has identified the systems and sharing arrangements that contain protected information that is or will be shared through the ISE.	For Information Sharing Council/Privacy Guidelines Committee member agencies, consider using the Green Pages as a starting point. The Green Pages are a self-identified list, initially requested by the Program Manager's Office (PM) in an effort to determine the scope of systems of records, databases, or data sets (herein referred to as systems) that contain terrorism information that would be shared in the Information Sharing Environment.
☐	2) Determine whether your agency has categorized its information systems/data sets, identifying which systems/data sets contain terrorism-related information? Did your agency use the PGC-approved Definitional Scope scheme, which categorizes information according to the adjacent column? If not, how is it categorized?	"Suggested Initial Steps for Applying the Information Sharing Environment Privacy Guidelines—Assessing Federal Agency Systems of Records": Found in **Appendix F** of this Workbook, this definitional scope paper suggests steps for applying the ISE Privacy Guidelines to agency systems ("systems" used herein refers to information systems, databases, and data sets, as appropriate) containing protected information within the scope of the ISE (also available at www.ise.gov). TRI is terrorism-related information as defined by the ISE Privacy Guidelines. For specific definitions, see the "ISE Privacy Guidelines Definitions," **Appendix H**. **Category I** •Systems that exclusively contain TRI •Initially identified on "Green Pages" •In ISE if system contains PI and is shared outside the agency **Category II** •Not designed to contain only TRI but may contain some TRI •Information is in the ISE if it is TRI, contains PI, and is shared outside agency •Non-TRI, if severable, is not subject to the ISE **Category III** •Does not contain any TRI •Administrative, regulatory information •Could become TRI if connection or link is made to TRI through the investigative/anlytical process and becomes Catagory I or Catagory II system PI.

TASKS/DECISION POINTS	STILL TO DO
STAGE II—Step 1: Identify systems and sharing arrangements in the ISE.	
1) Determine whether your agency has identified the systems and sharing arrangements that contain protected information that is or will be shared through the ISE.	
2) Determine whether your agency has categorized its information systems/data sets according to the Definitional Scope scheme.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
	STAGE II—Step 1: Identify systems and sharing arrangements in the ISE. (continued)	
☐	3) Determine whether your agency has identified the risk environment and associated risk-based protections that are warranted in the sharing of the information through the ISE.	Risk environment questions might include the following: a) Does the system/database contain sensitive information that is subject to specialized protections (e.g., personally identifiable information that reveals medical, financial, or religious information)? b) What specific protections must each category of information receive under legal, regulatory, or contractual obligations? c) What information privacy policies and practices are applied? d) Do exemptions from privacy protections that otherwise might apply continue to apply if the information is shared through the ISE? e) What is the likelihood that the data will be shared through the ISE? f) How could each category of information under consideration be exploited if it were inappropriately disclosed, accessed, or intercepted? g) What harms would result to an individual if protected information were inappropriately disclosed, accessed, or intercepted? h) What is the magnitude of the harm that could result from misuse of the information, whether the harm is to an individual, an organization, or larger interests, such as those of the United States? i) Who might be interested in inappropriately accessing, transmitting, or receiving each type of information, both inside and outside the agency maintaining it? j) If the information is shared with state agencies subject to state freedom of information or sunshine laws, might this information be made public? k) What harm might result from the inclusion or sharing of erroneous, misleading, or deficient information—to the individuals who are the subject of the information—to the agency?
	This is the list of systems/sharing arrangements to be assessed using your agency's ISE privacy policy to determine whether all the requirements are addressed or whether gaps need to be filled. The information in systems subject to the identified sharing arrangements should be handled consistently with all policies and procedures set forth by the agency's new/consolidated privacy policy. Where procedures do not satisfy the policy requirements, new measures must be implemented.	

TASKS/DECISION POINTS	STILL TO DO
STAGE II—Step 1: Identify systems and sharing arrangements in the ISE. **(continued)**	
3) Determine whether your agency has identified the risk environment and associated risk-based protections that are warranted in the sharing of the information through the ISE.	
This is the list of systems/sharing arrangements to be assessed using your agency's ISE privacy policy to determine whether all the requirements are addressed or whether gaps need to be filled. The information in systems subject to the identified sharing arrangements should be handled consistently with all policies and procedures set forth by the agency's new/consolidated privacy policy. Where procedures do not satisfy the policy requirements, new measures must be implemented.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**STAGE II—Step 2: Assess identified systems to ensure that the protected information is covered by the ISE privacy protection policy.**	
☐	1) Your agency may consider applying the risk environment questions in Step 1 to information currently shared in the ISE. If the information will continue to be shared, are special protections warranted?	
☐	2) For systems and sharing arrangements under consideration for sharing in the ISE, apply the risk environment questions in Step 1 to determine whether special protections are warranted.	

TASKS/DECISION POINTS	STILL TO DO
STAGE II—Step 2: Assess identified systems to ensure that the protected information is covered by the ISE privacy protection policy.	
1) Your agency may consider applying the risk environment questions in Step 1 to information currently shared in the ISE. If the information will continue to be shared, are special protections warranted?	
2) For systems and sharing arrangements under consideration for sharing in the ISE, apply the risk environment questions in Step 1 to determine whether special protections are warranted.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
	STAGE II—Step 2: Assess identified systems to ensure that the protected information is covered by the ISE privacy protection policy. (continued)	
☐	3) Your agency should examine practices relating to each system and sharing arrangement to determine whether they are consistent with the agency's written ISE privacy protection policy. Where procedures do not satisfy the policy requirements, new measures must be implemented.	In each case, evaluate whether: a) The **notice mechanisms** to ensure that information is handled in accordance with applicable legal requirements are applied to each system/sharing arrangement. b) The agency's **data-quality** procedures designed to ensure accuracy, timely correction (including court-expunged information), and appropriate retention of data are applied to each system/sharing arrangement, consistent with agency authorities. c) The agency's **data security** procedures designed to safeguard protected information are applied to each system/sharing arrangement, as appropriate. d) The agency's **enforcement** procedures designed to hold personnel accountable, ensure that staff are trained, and conduct compliance reviews and audits are applied to each system/sharing arrangement. e) The agency's **transparency** and **redress** procedures designed to inform the public of agency policies for addressing complaints regarding information under agency control are in place for each system/sharing arrangement and the procedures are effective. f) The agency has a procedure to trigger corrective procedures, including effective notice to receiving agencies upon discovery that protected information is erroneous or deficient and may cause harm if not corrected or deleted. g) If a terrorism-related information system contains state arrest records, does the agency have a procedure in place that defines how a federal agency recipient of information that is subject to court-ordered expungement will be notified of that order, to ensure that the information was deleted, and will notify any other ISE participants with which it has shared that information.
	Completing this step ensures that the agency's ISE privacy protection policy is applied to each system and sharing arrangement identified in the ISE.	

TASKS/DECISION POINTS	STILL TO DO
STAGE II—Step 2: Assess identified systems to ensure that the protected information is covered by the ISE privacy protection policy. (continued)	
3) Your agency should examine practices relating to each system and sharing arrangement to determine whether they are consistent with the agency's written ISE privacy protection policy. Where procedures do not satisfy the policy requirements, new measures must be implemented.	
Completing this step ensures that the agency's ISE privacy protection policy is applied to each system and the sharing arrangement identified in the ISE.	

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**STAGE II—Step 3: Protect systems and information shared in the ISE by conducting and documenting an agency's actions.**	
☐	1) Your agency may consider putting in place a policy that implements required protections for the system.	
☐	2) Your agency may consider putting in place procedures that address reporting, investigating, and responding to violations of privacy protection policies.	Having a reporting/notification procedure in place for violations of agency protection policies is expected to be a performance measurement for FY09.[3]
☐	3) Your agency may consider putting in place audit and enforcement mechanisms for systems implicated by the ISE.	The number of audits and enforcement actions is expected to be a performance measurement in FY09.[4]
☐	4) Your agency may consider providing ISE training to personnel authorized to access protected information; training should include procedures for reporting violations of agency privacy and civil liberties protection policies.	The number of personnel trained in the agency's ISE privacy protection policy is expected to be a performance measurement in FY09.[5]
☐	5) Your agency may consider establishing procedures to facilitate compliance with audits and review of agency ISE-related activities.	
☐	6) Your agency should designate an ISE privacy official[6] to receive reports (or copies) regarding alleged errors in protected information that originates from the agency.	
	Completion of this step should allow an agency to demonstrate its implementation and compliance with the ISE Privacy Guidelines.	

[3] Anticipated OMB requirement.
[4] Anticipated OMB requirement.
[5] Anticipated OMB requirement.
[6] Defined by section 12a of the ISE Privacy Guidelines to be the designated senior agency official with overall agency-wide responsibility for information privacy issues. An agency may decide to identify both a privacy official and a civil rights/civil liberties official.

TASKS/DECISION POINTS	STILL TO DO
STAGE II—Step 3: Protect systems and information shared in the ISE by conducting and documenting an agency's actions.	
1) Your agency may consider putting in place a policy that implements required protections for the system.	
2) Your agency may consider putting in place procedures that address reporting, investigating, and responding to violations of privacy protection policies.	
3) Your agency may consider putting in place audit and enforcement mechanisms for systems implicated by the ISE.	
4) Your agency may consider providing ISE training to personnel authorized to access protected information; training should include procedures for reporting violations of agency privacy and civil liberties protection policies.	
5) Your agency may consider establishing procedures to facilitate compliance with audits and review of agency ISE-related activities.	
6) Your agency should designate an ISE privacy official to receive reports (or copies) regarding alleged errors in protected information that originates from the agency.	
Completion of this step should allow an agency to demonstrate its implementation and compliance with the ISE Privacy Guidelines.	

Section 5. Ongoing Implementation and Compliance

COMPLETED	TASKS/DECISION POINTS	ADDITIONAL INFORMATION
☐	**Task—Has your agency submitted its written ISE privacy protection policy to the PGC?**	
☐	**Task—Will your agency make the policy available to the public to ensure transparency?**	
☐	**Task—How will your agency ensure that employees understand the policy?**	• What kind of training will your agency provide? • Must agency personnel acknowledge receipt of training on the policy?
☐	**Task—Has your agency established a process to ensure ongoing review of any new laws or policies so new requirements are appropriately incorporated into your ISE privacy protection policy?**	
☐	**Task—Has your agency established a process to ensure new or planned systems comply with your ISE privacy protection policy?**	
☐	**Task—Has your agency established a process for tracking ISE Privacy Guidelines performance measures?**	

TASKS/DECISION POINTS	STILL TO DO
Task—Has your agency submitted its written ISE privacy protection policy to the PGC?	
Task—Will your agency make the policy available to the public to ensure transparency?	
Task—How will your agency ensure that employees understand the policy?	
Task—Has your agency established a process to ensure ongoing review of any new laws or policies so new requirements are appropriately incorporated into your ISE privacy protection policy?	
Task—Has your agency established a process to ensure new or planned systems comply with your ISE privacy protection policy?	
Task—Has your agency established a process for tracking ISE Privacy Guidelines performance measures?	

Page intentionally left blank.

Appendix A
ISE Privacy Guidelines

*The ISE Privacy Guidelines were released on December 4, 2006.

Page is intentionally left blank.

Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment

1. Background and Applicability.

a. *Background*. Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE). Section 1 of Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, provides that, "[t]o the maximum extent consistent with applicable law, agencies shall … give the highest priority to … the interchange of terrorism information among agencies … [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities …." These Guidelines implement the requirements under the IRTPA and EO 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.

b. *Applicability*. These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

2. Compliance with Laws.

a. *General*. In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.

b. *Rules Assessment*. Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

(i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and

(ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.

c. Changes. If, as part of its rules assessment process, an agency:

(i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate develop policies and procedures to provide protections that address that issue;

(ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction;

(iii) identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review.

3. Purpose Specification.

Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below). Each agency shall adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected

information available through the ISE is consistent with the authorized purpose of the ISE.

4. Identification of Protected Information to be Shared through the ISE.

a. Identification and Prior Review. In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance with Laws) and Section 3 (Purpose Specification), each agency shall identify its data holdings that contain protected information to be shared through the ISE, and shall put in place such mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to these Guidelines before it is made available to the ISE.

b. Notice Mechanisms. Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:

(i) the information pertains to a United States citizen or lawful permanent resident;

(ii) the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and

(iii) there are limitations on the reliability or accuracy of the information.

5. Data Quality.

a. Accuracy. Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.

b. Notice of Errors. Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to

the other agency's ISE privacy official (the ISE privacy officials are described in section 12 below).

c. Procedures. Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:

(i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;

(ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and

(iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

6. Data Security.

Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.

7. Accountability, Enforcement and Audit.

a. Procedures. Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to:

(i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;

(ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies;

(iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and

(iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

b. Audit. Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

8. Redress.

To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

9. Execution, Training, and Technology.

a. Execution. The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs.

b. Training. Each agency shall develop an ongoing training program in the implementation of these Guidelines, and shall provide such training to agency personnel participating in the development and use of the ISE.

c. Technology. Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall consider and implement, as appropriate, privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

10. Awareness.

Each agency shall take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines.

11. Non-Federal Entities.

Consistent with any standards and procedures that may be issued to govern participation in the ISE by State, tribal, and local governments and private sector entities, the agencies and the PM-ISE will work with non-Federal entities seeking to

access protected information through the ISE to ensure that such non-Federal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines.

12. Governance.

a. *ISE Privacy Officials*. Each agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005), shall directly oversee the agency's implementation of and compliance with these Guidelines (the "ISE privacy official"). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency. The ISE privacy official role may be delegated to separate components within an agency, such that there could be multiple ISE privacy officials within one executive department. The ISE privacy official shall be responsible for ensuring that (i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these Guidelines, and (ii) changes are made as necessary. The ISE privacy official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's senior ISE official.

b. *ISE Privacy Guidelines Committee*. All agencies will abide by these Guidelines in their participation in the ISE. The PM shall establish a standing "ISE Privacy Guidelines Committee" to provide ongoing guidance on the implementation of these Guidelines, so that, among other things, agencies follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an inter-agency basis. The ISE Privacy Guidelines Committee is not intended to replace legal or policy guidance mechanisms established by law, executive order, or as part of the ISE, and will as appropriate work through or in consultation with such other mechanisms. The ISE Privacy Guidelines Committee shall be chaired by the PM or a senior official designated by the PM, and will consist of the ISE privacy officials of each member of the Information Sharing Council. If an issue cannot be resolved by the ISE Privacy Guidelines Committee, the PM will address the issue through the established ISE governance process. The ISE Privacy Guidelines Committee should request legal or policy guidance on questions relating to the implementation of these Guidelines from those agencies having responsibility or authorities for issuing guidance on such questions; any such requested guidance shall be provided promptly by the appropriate agencies. As the ISE governance process evolves, if a different entity is established or identified that could more

effectively perform the functions of the ISE Privacy Guidelines Committee, the ISE Privacy Guidelines Committee structure shall be modified by the PM through such consultation and coordination as may be required by the ISE governance process, to ensure the functions and responsibilities of the ISE Privacy Guidelines Committee remain priorities fully integrated into the overall ISE governance process.

c. *Privacy and Civil Liberties Oversight Board*. The Privacy and Civil Liberties Oversight Board (PCLOB) should be consulted for ongoing advice regarding the protection of privacy and civil liberties in agencies' development and use of the ISE. To facilitate the performance of the PCLOB's duties, the ISE Privacy Guidelines Committee will serve as a mechanism for the PCLOB to obtain information from agencies and to provide advice and guidance consistent with the PCLOB's statutory responsibilities. Accordingly, the ISE Privacy Guidelines Committee should work in consultation with the PCLOB, whose members may attend Committee meetings, provide advice, and review and comment on guidance as appropriate.

d. *ISE Privacy Protection Policy*. Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines. Agencies should consult with the ISE Privacy Guidelines Committee as appropriate in the development and implementation of such policy.

13. General Provisions.

a. Definitions.

(i) The term "agency" has the meaning set forth for the term executive agency" in section 105 of title 5, United States Code, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government accountability Office.

(ii) The term "protected information" has the meaning set forth for such term in paragraph 1(b) of these Guidelines.

(iii) The terms "terrorism information," "homeland security information," and "law enforcement information" are defined as follows:

"Terrorism information," consistent with section 1016(a)(4) of IRTPA means all relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of

domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, (C) communications of or by such groups or individuals, or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

"Homeland security information," as derived from section 482(f)(1) of the Homeland Security Act of 2002, means any information possessed by a Federal, State, local, or tribal agency that relates to (A) a threat of terrorist activity, (B) the ability to prevent, interdict, or disrupt terrorist activity, (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization, or (D) a planned or actual response to a terrorist act.

"Law enforcement information" for the purposes of the ISE means any information obtained by or of interest to a law enforcement agency or official that is (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

b. The treatment of information as "protected information" under these Guidelines does not by itself establish that the individual or entity to which such information pertains does in fact have information privacy or other legal rights with respect to such information.

c. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide the cooperation, assistance, and information necessary for the implementation of these Guidelines.

d. These Guidelines:

(i) shall be implemented in a manner consistent with applicable laws and executive orders, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;

(ii) shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;

(iii) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(iv) are intended only to improve the internal management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

Page is intentionally left blank.

Appendix B
2006 Interagency Compilation of Federal Privacy and Civil Liberties Policies That Impact Information Sharing

*This document was prepared by the Interagency Working Group tasked with preparing the ISE Privacy Guidelines. The research identified 109 sets of rules set forth herein. This list is not exhaustive but may serve as a starting point for agencies to identify the laws and policies applicable to ISE information.

Page intentionally left blank

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
1	**U.S. Constitution—especially Fourth and Fifth Amendments**	Constitution	Provides fundamental individual protections vis-à-vis government.	Yes.	Information sought/used by USG.	WMD 9.4, Markle, TIA, CDT
2	**Information Sharing, section 1016 of IRTPA, 6 U.S.C.§ 485**	Statute	Establishes "information sharing environment."	Yes—Requires guidelines for protection of privacy and civil liberties.	Terrorism information.	WMD 9.4, AT
3	**Privacy and Civil Liberties Oversight Board, section 1061 of IRTPA, 5 U.S.C. § 601 note**	Statute	Establishes Board.	Yes—Provides Board with access, advice, oversight authorities, and responsibilities relating to privacy and civil liberties.	"[R]elated to efforts to protect the nation from terrorism." Includes terrorism information.	WMD 9.4, AT
4	**National Security Act of 1947, as amended by IRTPA, section 102A and 103A, 50 U.S.C. § 403-1, 3d**	Statute	Various provisions authorizing/requiring sharing.	Yes—Creation of Civil Liberties Protection Officer position.	National intelligence.	WMD 9.4
5	**Privacy Act, 5 U.S.C. §552a, as amended**	Statute	Privacy Act sets collection, maintenance, and disclosure conditions; access and amendment rights and notice and record-keeping requirements with respect to personally identifiable information retrieved by name or identifier. Computer matching provisions (amending Privacy Act) provide a framework for the intra- and interagency comparison of electronic personnel and benefits-related information systems.	Yes, see summary.	Information about a citizen or LPR that contains name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger- or voiceprint or photograph.	ISWG, OMB, CMS/LGL, Markle, TIA, CDT

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
6	**E-Government Act of 2002**	Statute	Section 208 requires agencies to analyze (i) how they handle personally identifiable information used in electronic business processes and (ii) where protecting privacy demands modifications to the business process or information system (i.e., Privacy Impact Assessment).	Yes—Requires PIAs and Web site privacy notices; exemption for "national security systems." Also, modification or waiver of PIA is permitted "for security reasons or to protect classified, sensitive, or private information contained in an assessment."	Information in identifiable form that is collected, maintained, or disseminated by information technology. Does not apply to "national security systems." "Identifiable form" means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.	OMB, CRS, Markle
7	**Freedom of Information Act, 5 U.S.C. § 552**	Statute	Provides for the disclosure of agency records to the public, subject to certain exemptions.	Yes—Contains exemptions relating to personal privacy information—exemptions 6 and 7(c).	Agency records.	WMD 9.4, ISWG, CRS, CDT,TIA
8	**Foreign Intelligence Surveillance Act (electronic surveillance, physical search, pen registers, business records)**	Statute	Governs collection, retention, dissemination of foreign intelligence information via electronic surveillance, physical search, business records, pen register trap/trace. Requires AG-approved minimization procedures to protect USP information.	Yes—Collection predicates, minimization requirements.	Information acquired under FISA (electronic surveillance, physical search, pen register/trap trace, business records).	ISWG, WMD 9.4, CRS, Markle, TIA, CDT

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
9	**Pen Registers and Trap and Trace Devices Act, 18 U.S.C. § 3121 et seq.**	Statute	Provisions on collecting information via pen registers and trap/trace devices.	Yes—Collection predicate.	Communications addressing information.	CRS, TIA
10	**National Security Act of 1947, USA PATRIOT Act and Homeland Security Act amendments, 50 U.S.C. § 403-5b and 5d**	Statute	USA PATRIOT Act and Homeland Security Act amendments authorizing and requiring sharing of foreign intelligence collected from criminal investigations.	No.	Information acquired in the course of criminal investigations.	ISWG, CRS
11	**USA PATRIOT Act, sections 203(a) and (b)—Authority to Share Grand Jury Information; Electronic, Wire, and Oral Interception Information**	Statute	Amends Rule 6 to authorize sharing of grand jury information in matters involving FI and CI; adds (6) to 18 U.S.C. § 2517, authorizing sharing of information collected via authorized interception with federal law enforcement, intelligence, and other national security officials.	Yes—Use limited to official duties; GJ info requires filing under seal; sharing of USP information subject to AG guidelines.	Information acquired via Grand Jury subpoena or Title III/ECPA.	LSG, CRS, TIA
12	**Homeland Security Act of 2002, sections 895 and 896, Authority to Share Grand Jury Information; Electronic, Wire, and Oral Interception Information**	Statute	Authorizes sharing of grand jury information for terrorism prevention, etc.; adds (7) and (8) to 18 U.S.C. § 2517, authorizing sharing of information collected via authorized interceptions with federal/state/local/foreign officials.	Yes—Use limited to official duties, pursuant to joint AG/DCI guidelines.	Same as above.	
13	**Homeland Security Act of 2002, section 892, Facilitating Homeland Security Information Sharing Procedures**	Statute	Under procedures prescribed by the President, requires sharing of homeland security information across federal government and with state/local personnel.	Yes—Information sharing system must ensure confidentiality of information and protect constitutional and statutory rights of individuals.	Homeland security information.	ISWG, CRS, TIA

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
14	**Counterintelligence Access to Telephone Toll and Transactional Records, 18 U.S.C. § 2709**	Statute	Access to subscriber information, toll billing records, and electronic communication transactional records by FBI.	Yes—Requires certification that information is relevant to authorized CI or CT investigation.	Telecommunications subscriber information, toll billing records, and electronic communication transaction records.	CMS/LGL, Markle
15	**USA PATRIOT Act, National Security Letter authorities**	Statute	USA PATRIOT Act amendments included clarifications/enhancements to "national security letter" authority under various other statutes.	Yes—Requires relevance to an ongoing terrorism investigation.	Information relevant to a terrorism investigation.	CDT (Others included this in references to the underlying statutes.)
16	**Privacy Protection Act, 42 U.S.C. § 2000aa**	Statute	Prohibits seizure of work product and other documentary materials in exercise of First Amendment rights, subject to certain exceptions.	Yes—Provides protection for First Amendment rights.	Work products and other documentary materials.	G1a
17	**Posse Comitatus Act, 18 U.S.C. § 1385**	Statute	Prohibits the Army and Air Force from executing U.S. laws.	Yes—Prevents military from acting in law enforcement capacity vis-à-vis civilians.	Military.	ISWG, LSG
18	**Use of Information Collected During Military Operations, 10 U.S.C. § 371**	Statute	Requires DoD to share relevant information with civilian law enforcement officials that may be relevant to a violation of any federal or state law in their jurisdiction.	Yes—Sharing must be in accordance with applicable law.	Information collected during military operations.	LSG

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
19	**Tax Return Information, 26 U.S.C. § 1063**	Statute	Prohibits disclosure of tax return or return information (very broad definition) by any officer or employee of the United States, state or local law enforcement agency, local child support enforcement agency, or "other person" as defined, except as provided by the provision.	Two of the exceptions apply to the release of terrorist-related information to federal intelligence agencies. Pursuant to section 6103(i)(7)(B), the Secretary of the Treasury may, upon written request, disclose return information (other than information furnished by or on behalf of the taxpayer directly) to federal intelligence agencies that are engaged in the collection or analysis of intelligence and counterintelligence information or investigation concerning any terrorist incident, threat, or activity. In addition, section 6103(i)(7)(C) permits the disclosure of returns and return information to federal intelligence agencies pursuant to an ex parte order by a federal judge. The unauthorized disclosure of returns and return information is subject to civil and criminal sanctions under IRC sections 7431 and 7213. Section 6103 does not differentiate between U.S. and non-U.S. persons with respect to the sharing or release of taxpayer information.	Tax return information.	OMB, WMD 9.4, CRS, TIA
20	**Social Security Information, 42 U.S.C. § 1306**	Statute	Governs use and disclosure of social security information.	Yes—Prohibits disclosure except as provided by law and regulation.	Social security information.	TAPAC

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
21	**PL 109-115, Transportation, Treasury, HUD, etc., Act, 2006, 119 Stat. 2503**	Statute	Provision in annual agency appropriation act permanently applicable throughout the government.	Yes—Section 832 prohibits any federal agency from using appropriated funds (funds "made available in this or any other Act") to monitor an individual's use of a federal government Internet site and also prohibits agency from entering into any agreement with a third party to obtain or aggregate personally identifiable information relating to an individual's access to or use of any nongovernmental Internet site. Does not apply to voluntary submission of personally identifiable information.	Personally identifiable information from Web site usage.	OMB
22	**Census Bureau Information, 13 U.S.C. § 9**	Statute	Prohibits the use, publication, or examination of any information collected by the U.S. Census Bureau.	Yes—Narrow exceptions—no law enforcement/national security or similar exceptions.	Census data.	CRS, TIA
23	**Family Educational Rights and Privacy Act ("Buckley Amendment"), 20 U.S.C. § 1232g**	Statute	Requires notice to student/parents if educational records are disseminated—exceptions for investigation of terrorism, with court order on application of AG showing relevance to investigation (1232g(j)).	Yes.	Educational records.	WMD 9.4, CMS/LGL, CRS, Markle, TIA, CDT
24	**Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq.**	Statute	Restricts use and disclosure of financial records of customers by financial institutions.	Yes—Contains exception for voluntary responses to requests from government authority authorized to conduct CI or FI activities and for mandatory responses to FBI requests. 12 U.S.C. § 3414.	Financial records.	WMD 9.4, CMS/LGL, CRS, Markle, TIA, CDT

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
25	**Fair Credit Reporting Act, 15 U.S.C. § 1681**	Statute	Restricts use and disclosure of credit report information (1681f) with exception for header information to government agencies and to government agencies for counterterrorism purposes (1681v).	Yes—Contains exception for counterterrorism purposes, with certification.	Credit report information.	WMD 9.4, CMS/LGL, CRS, Markle, TIA, CDT
26	**Gramm-Leach-Bliley Financial Modernization Act, 12 U.S.C. § 1811 note**	Statute	Governs collection, sharing of customer information by financial institutions.	Yes—Requires notice, choice, and security safeguards. General exception for sharing in accordance with RFPA and to LE agencies, etc. 15 U.S.C. § 6802(e).	Financial information.	CMS/LGL, CRS, Markle, TIA, CDT
27	**Bank Secrecy Act of 1970, 12 U.S.C. §§ 1892b and 1951-59, and 31 U.S.C. §§ 5311-22, and its major component, the Currency and Foreign Transactions Reporting Act, 31 U.S.C. §§ 5311-22 (anti-money laundering laws); also FinCEN, 31 USC 310**	Statute	Requires filing of Suspicious Activity Reports and other anti-money laundering measures and reporting by "financial institutions," broadly defined, and requires DOT to promulgate regulations to ensure that adequate records are maintained of transactions that have a high degree of usefulness in investigatory proceedings. Also establishes FinCEN. The regulations implementing the BSA are set forth at 31 CFR Part 103. In particular, 31 U.S.C. § 5319 provides for the sharing of information with the Intelligence Community, and FinCEN's regulation covering procedures for information sharing authorizes the sharing of BSA information with members of the Intelligence Community for a national security purpose. See 31 CFR 103.53(d).	Yes—Reports shared with intelligence agencies must be consistent with purpose of subchapter, which includes providing information for FI, CI, and counterterrorism. Treasury regulations must be consistent with Privacy Act and RFPA and must establish guidelines for access and use.	Financial information.	WMD 9.4, CRS, TIA, CDT
28	**Title III and Electronic Communications Privacy Act, 18 U.S.C. § 2511 et seq., 2701 et seq.**	Statute	Restricts the interception of electronic communications and access to stored communications.	Yes.	Electronic and stored communications.	WMD 9.4, CMS/LGL, CRS, Markle, TIA, CDT

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
29	**Telecommunications Act of 1996, 47 U.S.C. § 153 et seq.**	Statute	Governs provision of telecommunications services.	Yes—section 222 contains certain privacy provisions.	Customer proprietary network information.	CMS/LGL, CRS, TIA
30	**Cable Communications Policy Act of 1984, 47 U.S.C. § 521 et seq.**	Statute	Section 631 (47 U.S.C. § 551) covers subscriber privacy—provides for notice, consent, limits on disclosure, government access only pursuant to court order with clear and convincing standard.	Yes.	Cable usage information.	CMS/LGL, CRS, Markle, TIA
31	**Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq.**	Statute	Restricts use and disclosure of state DMV records, with multiple exceptions, including for government official use.	Yes.	DMV records.	CMS/LGL, CRS, TIA
32	**Video Privacy Protection Act of 1988, 18 U.S.C. § 2710**	Statute	Prohibits disclosure of videotape rental records.	Yes.	Videotape rental records.	CMS/LGL, CRS, Markle, TIA
33	**Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320**	Statute	Multiple provisions regarding health insurance portability and fraud.	Yes—Section 264 provides that HHS must promulgate standards with respect to privacy of individually identifiable health information, which were issued as 45 CFR Part 164. The Privacy Rule applies to health care entities and contains an exemption for disclosure to authorized federal officials for the conduct of lawful intelligence, CI, and national security activities. 45 CFR 164.512.	Individually identifiable health information.	CMS/LGL, CRS, Markle, TIA, CDT

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
34	**Immigration—Application for Visas, 8 U.S.C. § 1202**	Statute	Various immigration provisions.	Yes—Prohibits disclosure of U.S. Department of State records relating to issuance or refusals of permits for entry to the U.S. Such records are only to be used for administration of immigration, nationality, and other U.S. laws, and otherwise may only be disclosed at the discretion of the Secretary of State to courts and foreign governments under specified circumstances.	Immigration records—visa information.	FGI, CRS
35	**Immigration—Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. § 1367**	Statute	Various immigration provisions.	Yes—Prohibits disclosure of any information that relates to a person who has filed a claim under the Violence Against Women Act where claim is pending or approved. Exceptions include AG providing for law enforcement purposes.	Immigration records—Claim information filed under Violence Against Women Act.	FGI
36	**Immigration—Legalization/Seasonal Agricultural Work claims, 8 U.S.C. § 1255a**	Statute	Immigration provisions.	Yes—Prohibits disclosure of information relating to Legalization/Seasonal Agricultural Work claims, with limited law enforcement exception.	Immigration records—Claim information relating to Legalization/ Seasonal Agricultural Work status.	FGI
37	**Immigration—T Visas and U Visas, section 701 of PL 106-386**	Statute	Immigration provisions.	Yes—Restricts disclosure of information relating to trafficking victims (T visas) and victims of crimes (U visas). 8 CFR 214.11(e) enables DHS to provide for law enforcement of those crimes.	Immigration records—victims of crime.	FGI

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
38	**Immigration—Temporary Protected Status, 8 U.S.C. § 1254a and 8 CFR 244.166**	Statute	Immigration provisions.	Yes—Restricts DHS disclosure of information relating to temporary protected status of an alien, except for disclosure in course of official duties or for enforcement of INA.	Immigration records—temporary protected status.	FGI
39	**Passenger Manifest Reporting Requirements, 8 U.S.C. § 1221, 19 CFR 4.7**	Statute	Requirement that aircraft and vessels report to CBP their passenger manifests before arrival in or departure from the United States.	No.	Passenger manifests.	CDT
40	**TSA—Research and Development Activities, 49 U.S.C. § 40119**	Statute	Research and development to protect passengers and property against piracy, criminal violence, and terrorism.	Yes—Requires Secretary of Transportation to prescribe regulations for restricting disclosures that would constitute an unwarranted invasion of privacy.	TSA R&D information.	FGI
41	**Consolidated Appropriations Act of 2005**	Statute	Requires chief privacy officers and contains other related privacy provisions. Note: Applicability unclear to agencies outside of appropriation.	Yes.	Information in possession of covered federal agencies.	OMB
42	**Federal Trade Commission Act, 15 U.S.C. § 41-58**	Statute	Prohibits unfair or deceptive trade practices and provides FTC with enforcement authority.	Yes—FTC has enforced act vis-à-vis private sector violations of published privacy policies.	Private sector data.	CRS
43	**Children's Online Privacy Protection Act, 15 U.S.C. § 6501**	Statute	Governs Web site collection of information from minors.	Yes.	Web site data collected from children.	CRS, TIA
44	**Child Victims' and Child Witnesses' Rights, 18 U.S.C. § 3509**	Statute	Nondisclosure provisions for child victims and witnesses.	Yes.	Child victim/witness data.	TIA
45	**Federal Juvenile Delinquency Act, 18 U.S.C. § 5031 et seq.**	Statute	Nondisclosure provisions for juvenile delinquency records.	Yes—Law enforcement exception.	Juvenile delinquency records.	TIA

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
46	**Acquisition, Preservation, and Exchange of Identification Records and Information**	Statute	Requires AG to acquire, collect, classify, and preserve identification, criminal identification, crime and other records and exchange with other authorized officials of federal and state agencies for official use.	Yes—Exchange cancelled if recipient shares outside of organization.	Criminal identification information in possession of DOJ.	TIA
47	**Alcohol and Drug Abuse Records, 42 U.S.C. § 290dd-2, and Drug Test Results, PL 100-71, section 503**	Statute	Limits disclosure of alcohol and drug abuse patient records and drug test results.	Yes—Limited exceptions.	Medical information.	TIA
48	**Americans with Disabilities Act and the Rehabilitation Act**	Statute	Improper release of medical information may be considered an act of disability discrimination.	Yes.	Medical information.	TIA
49	**Federal Rule of Criminal Procedure 32**	Federal Rule	Probation officer presentence reports.	Yes—No disclosure without defendant consent, guilty plea, or conviction.	Criminal records.	TIA
50	**EO 12333, United States Intelligence Activities**	Executive Order	Governs intelligence activities.	Yes—Provides rules for collection, retention, and dissemination of U.S. person information.	U.S. person information.	All
51	**EO 13311, Homeland Security Information Sharing**	Executive Order	Assigns to DHS the President's responsibility for procedures under 892(a)(1) of Homeland Security Act.	No.	Homeland security information.	CMS/LGL, CRS
52	**EO 13388, Further Strengthening the Sharing of Terrorism Information Sharing to Protect Americans**	Executive Order	Provides for information sharing to protect against terrorism.	Yes—Requires that agencies give the "highest priority" to, inter alia, the interchange of terrorism information, and in doing so, to protect the freedom, information privacy, and other legal rights of Americans.	Terrorism information.	AT
53	**HSPD 6**	Presidential Directive	Establishes terrorist watch-list framework.	Yes—Requires safeguards for USP information.	Terrorist information.	WMD 9.4

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
54	**Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation.**	AG Memo, Sept 2002	Provides guidance to federal law enforcement for sharing foreign intelligence with the Intelligence Community. This memorandum applies to the U.S. Department of Homeland Security, U.S. Department of Justice, and other federal entities having law enforcement responsibilities.	Compilation did not refer to specific privacy provisions—not further reviewed.	Law enforcement information.	ISWG, CMS/LGL, TIA
55	**Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons [Section 203 Guidelines].**	AG Memo, Sept 2002	Specifies procedures for the handling and labeling of information that identifies U.S. persons when sharing such information with the Intelligence Community.	Yes—This memorandum restricts the ability to share certain types of information afforded by the USA PATRIOT Act until there is enough information available to determine whether or not the subject of the intercepted information is a U.S. citizen.	Law enforcement information.	ISWG, CMS/LGL, AT

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
56	**Guidelines for FBI National Security Investigations and Foreign Intelligence Collection**	AG Guidelines Oct 2003	Guidelines state as a "general principle" that "the FBI shall provide information expeditiously to other agencies in the Intelligence Community, so that these agencies can take action in a timely manner to protect the national security in accordance with their lawful functions." AG Guidelines also state that consistent with this overriding priority, the FBI shall act in a manner to protect, to the greatest extent possible . . . other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information. Affirms the MOU on Homeland Security Information Sharing. Authorizes sharing with foreign authorities when in the national security interest but requires that the FBI consider the reasonably expected effect on any identifiable U.S. person.	Yes—FBI counterintelligence and foreign intelligence information collected under the AG Guidelines, including information acquired in "National Security Investigations" concerning U.S. persons, may be shared with other IC components so they can determine relevance to their responsibilities. However, sharing may be limited to protect security, operational, and prosecutorial interests. In addition, sharing with foreign authorities requires considering the effect on any identifiable U.S. person.	FBI foreign intelligence and counterintelligence .	ISWG, AT
57	**Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations**	AG Guidelines May 2002	Governs FBI investigations of terrorism enterprises.	Yes—USP rules.	FBI information.	CRS, TAPAC, TIA
58	**Guidelines Applicable to FBI Foreign Counterintelligence Investigations**	AG Guidelines	Governs FBI foreign CI investigations.	Yes.	FBI information.	TIA

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
59	**DOJ—Criminal Intelligence System Operating Policies, 28 CFR Part 23**	DOJ Regulations	Provisions for ensuring that all criminal intelligence systems operating under Omnibus Crime Control and Safe Streets Act are utilized in conformance with the privacy and constitutional rights of individuals.	Yes—28 CFR 23.20 sets forth "operating principles" to protect privacy and constitutional rights, such as ensuring information is based on reasonable suspicion, no information is in violation of law, dissemination based on need to know, etc.	Criminal intelligence.	G1a
60	**DOJ—*The National Criminal Intelligence Sharing Plan***	DOJ Guidance	The *National Criminal Intelligence Sharing Plan* ("Plan") is a formal intelligence sharing initiative that addresses the security and intelligence needs recognized after the tragic events of September 11, 2001. It describes a nationwide communications capability that will link together all levels of law enforcement personnel, including officers on the streets, intelligence analysts, unit commanders, and police executives for the purpose of sharing critical data.	Yes—Contains guidance for creating privacy policies and for protecting privacy, civil liberties, and civil rights during information sharing.	Criminal intelligence.	G1a
61	**DOJ—Justice Information Privacy Guideline**	DOJ Guidance	Referenced in the Plan—a guideline for developing, drafting, and assessing privacy policy for justice information systems (criminal and civil justice systems across the board, not DOJ-centric).	Yes—Provides guidance on developing privacy policy for civil and criminal justice systems.	Information in civil and criminal justice systems.	G1a
62	**DOJ—*Privacy and Civil Liberties Policy Development Guide and Implementation Templates***	DOJ Guidance	Developed by Global Privacy and Information Quality Working Group of DOJ's Global Justice Information Sharing Initiative.	Yes—Provides guidance on developing privacy policies to protect personal information in a sharing environment.	Information in civil and criminal justice systems.	G1a

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
63	**DOJ/DHS—*Fusion Center Guidelines***	DOJ-DHS Guidance	Guidelines for establishing and operating fusion centers at the local, state, tribal, and federal levels.	Yes—Guideline 8 is to develop, publish, and adhere to a privacy and civil liberties policy. Provides guidance on developing policies—refers to Justice Information Privacy Guideline.	Law enforcement intelligence.	G1a
64	**National Instant Criminal Background Check System, DOJ Regulations, 28 CFR Part 25**	DOJ Regulations	Procedures for implementing the Brady Act referencing instant criminal background checks for firearms transfers.	Yes—Access prohibited for any purpose other than issuance of firearms licenses and enforcement of the Gun Control Act.	Criminal background records.	WMD 9.4
65	**DOJ/FBI—Production or Disclosure of Material, 28 CFR Part 16**	FBI Regulations	Regulations for disclosing FBI records, including under Privacy Act, in litigation, and on request of subject.	Yes.	Law enforcement.	G1a
66	**FBI Policy for Law Enforcement Sensitive Marking, Letter From FBI Deputy Director to Deputy Secretary of Defense**	FBI Policy	The "Law Enforcement Sensitive" (LES) marking indicates that information was compiled for law enforcement purposes and should be afforded appropriate security to protect specified law enforcement interests. Such information generally is not classifiable. It is to be entrusted only to those persons within an agency who have demonstrated a legitimate need to know the information. It is to be safeguarded in accordance with U.S. Department of Justice requirements for information marked "Limited Official Use" and is the type of information exempt from disclosure under FOIA Section 552(b).	Compilation did not refer to specific privacy provisions—not further reviewed.	Law enforcement information.	WMD 9.4
67	**FBI Standard FISA Minimization Procedures (various)**	AG-Approved Procedures	Sets forth procedures for minimizing U.S. person information collected under FISA.	Yes.	Intelligence information collected under FISA.	WMD 9.4

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
68	**Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the U.S. Department of Homeland Security Concerning Information Sharing**	MOU March 2003	Prescribes policies and procedures for sharing terrorism information.	Yes—"All information sharing pursuant to this Agreement shall be consistent with applicable privacy laws."	Terrorism information.	ISWG, WMD 9.4, CMS/LGL
69	**Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism (TSC MOU); and Addendum A**	MOU	Prescribes policies and procedures for terrorist screening information and the Terrorist Screening Center.	Yes—Procedures must be developed to address repeated misidentification, regularly correct information, and protect personal privacy.	Terrorist information.	WMD 9.4
70	**DCID 2/5—TTIC**	DCI Directive	Establishes TTIC.	Yes—Requires agency assignees to continue to comply with their own legal authorities and restrictions and all applicable statutes and EOs, "including those relating to the protection of Constitutional rights and privacy."	Terrorist threat-related information.	CMS/LGL
71	**DCID 8/1—Information Sharing**	DCI Directive	Requires expanded information sharing by Intelligence Community.	No.	Intelligence information.	CMS/LGL
72	**DoD 5240.1, DoD Intelligence Activities**	DoD Directive	Governs DoD Intelligence Activities.	Yes—Lays out general governing principles/restrictions; refers to 5240.1-R.	Intelligence information.	ISWG

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
73	**DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons [also note classified SIGINT annex]**	DoD Directive	Limits and provides procedures for collection, retention, use, and dissemination of information about U.S. persons.	Yes—Imposes strict limits on information that may be collected or retained about U.S. persons. Severely limits information that can be received from law enforcement and the fluidity with which information can be shared. Permitted to disseminate to: (1) DoD employee needing it for duties, (2) appropriate F/S/L law enforcement, (3) agency within Intelligence Community, (4) federal agency authorized to receive in relation to its duties, and (5) foreign government authorized under agreement. May also share incidentally acquired information with F/S/L law enforcement re: violation of law.	Intelligence information.	ISWG
74	**DIA Regulation 60-4 Procedures Governing DIA Intelligence Activities That Affect U.S. Persons**	DIA Regulation	Outlines authorities and procedures in conducting intelligence activities that may affect U.S. persons, to include identifying and reporting questionable activities.	Yes—Restricts the collection, retention, and dissemination of information concerning U.S. persons.	Intelligence information.	ISWG
75	**USSID 18—Legal Compliance and Minimization Procedures**	NSA Regulation	Governs collection, retention, and dissemination of information by NSA.	Yes.	Intelligence information.	ISWG, WMD 9.4
76	**Standard Minimization Procedures for NSA Electronic Surveillances [FISA]**	NSA Regulation	Required by FISA.	Yes—Procedures for minimizing USP information under FISA.	FISA information.	WMD 9.4

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
77	**DCI Memorandum on Procedures for Dissemination of Intelligence Referring to Members of Congress and Their Staffs ("Gates Procedures")**	DCI Directive	Restrictions on dissemination of identity information re Congress members/staffs.	Yes.	Intelligence information.	WMD 9.4
78	**Imagery Policy Series**	NGA Regulation	Imagery guidelines and restrictions.	Document referenced in compilation but not described—not further reviewed.	Imagery.	ISWG
79	**DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations Not Affiliated With the Department of Defense**	DoD Directive	Applies to nonintelligence DoD elements. Sets out numerous restrictions pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with the U.S. Department of Defense.	Yes—Prohibits certain types of otherwise legal collection, storage, and dissemination of information. Requires high-level approval of certain other types.	Information in possession of DoD.	ISWG
80	**DoD Directive 1304.23, Acquisition and Use of Criminal History Record Information by the Military Services, November 16, 1994**	DoD Directive	Criminal background information on DoD applicants.	Yes—Requires confidentiality of records, use only for applicant review purposes.	Criminal background records.	G1a
81	**DoD Directive 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, November 3, 2005**	DoD Directive	Rules for intelligence interrogations, etc.	Yes—Medical information of detainees must be handled with respect for patient privacy.	Medical information of detainees.	G1a
82	**DoD Directive 5400.11, DoD Privacy Program (see also 5400.11-R)**	DoD Directive	Policy and procedures to implement Privacy Act to maintain privacy of personal information on individuals held in a system of records maintained by a Component.	Prohibits release of personal information on individuals held in a system of records maintained by a Component, with limited exceptions [does not refer to 5240.1-R].	DoD Privacy Act information.	ISWG

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
83	**DoD Directive 5525.5, DoD Cooperation With Civilian Law Enforcement Officials**	DoD Directive	Policy encouraging cooperation with F/S/L law enforcement.	Refers to 5420.1-R and 5400.11, among others.	Information in possession of DoD.	ISWG
84	**DoD Directive 2000.12, DoD Anti-Terrorism Program, 18 Aug 2003**	DoD Directive	Establishes responsibilities within DoD regarding anti-terrorism; inter alia, requires "fusing" of information and "suspicious activity reporting" from law enforcement, CI, and other sources.	No.	Information in possession of DoD.	G1a
85	**DoD Regulation 6025.18-R, DoD Health Information Privacy Regulations, January 24, 2003**	DoD Regulation	Implements HIPAA privacy rule.	Yes—Governs use and disclosure of health information.	Personally identifiable health information.	G1a
86	**DoD—Joint Pub (JP) 3-07.2 Joint Tactics, Techniques, and Procedures for Anti-Terrorism, 1998**	DoD Guidance	Provides guidance for DoD anti-terrorism measures.	Yes—Contains legal guidance for use of military in anti-terrorism situations, including legal guidance for domestic situations.	Military.	G1a
87	**DoD Strategy for Homeland Defense and Civil Support**	DoD Strategy	Supports homeland defense.	Yes—Actions must be consistent with privacy protections and constitutional authorities.	Information in possession of DoD.	G1a
88	**AF Instruction 14-104, Oversight of Intelligence Activities**	Air Force Instruction	U.S. Air Force regulation for intelligence oversight.	Yes—USP rules.	USP information.	WMD 9.4
89	**AF Policy Directive—AFPD 71-1, Criminal Investigations and Counterintelligence**	Air Force Policy	Governs criminal investigations and CI to protect AF personnel and facilities.	Yes—Reference to USP rules.	Information in possession of USAF.	G1a
90	**Army Regulation 381-10, U.S. Army Intelligence Activities**	Army Regulation	Army regulation for intelligence activities.	Yes—USP rules.	USP information.	WMD 9.4

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
91	**Secretary of the Navy Instruction 381-10, Oversight of Intelligence Activities Within the Department of the Navy**	Navy Instruction	Navy regulation for intelligence oversight.	Yes—USP rules.	USP information.	WMD 9.4
92	**CIA HR 7-1, Law and Policy Governing the Conduct of Intelligence Activities**	CIA Regulation and AG Guidelines	Classified regulation—contains AG guidelines under EO 12333 and imposes other restrictions.	Yes.	USP information.	CMS/LGL
93	**Department of Energy Procedures for Intelligence Activities (with supplements)**	DOE Regulation and AG Guidelines	Contains AG guidelines under EO 12333.	Yes.	USP information.	WMD 9.4
94	**OMB—Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948 (July 9, 1975)**	OMB Guidelines	Amplifies on all Privacy Act terms and provisions, including limitations on and requirements for disclosure of identifiable information outside the agency.	Yes.	Privacy Act information.	OMB
95	**OMB—Privacy Act Guidance—Update (May 24, 1985)**	OMB Guidelines	Supplemental guidance addressing use of Privacy Act information in the litigation context and relationship of Privacy Act to FOIA (nonconsensual disclosure of information where FOIA requires).	Yes.	Privacy Act information.	OMB
96	**OMB—Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 FR 25818 (June 16, 1989)**	OMB Guidelines	Explains content of and procedures for conducting cost-benefit analyses and publishing interagency agreements preliminary to conducting computer matches.	Yes.	Privacy Act information.	OMB

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
97	**OMB—Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act of 1974, 56 FR 18599 (April 23, 1991)**	OMB Guidelines	Addresses verification procedures (due process requirements) preliminary to decision making about individual rights, benefits, or privileges based on information derived from computer matching activities.	Yes.	Privacy Act information.	OMB
98	**OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, Appendix 1 (November 28, 2000)**	OMB Guidelines	Amplifies on statutory (Privacy Act) requirements for publication of Privacy Act Systems of Records Notices and Computer Matching Agreements that implicate disclosure of records outside the agency.	Yes.	Privacy Act information.	OMB
99	**OMB Circular A-16, Coordination of Geographic Information and Related Spatial Data Activities (August 19, 2002) (incorporates EO 12906)**	OMB Guidelines	Describes the responsibility of agencies to collect, share, and disseminate spatial data among all levels of government.		Special data.	OMB
100	**OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (OMB Memorandum 03-22, February 2004)**	OMB Guidelines	Articulates requirement to conduct or update Privacy Impact Assessment when a system change creates new privacy risks, such as application of new technologies; matching, merging, or centralization of databases; incorporation of commercial source information; and new interagency uses (e.g., where agencies work on shared functions involving significant new uses or exchanges of information in identifiable form, alternation of business process, and alteration in character of data).	Yes.	E-Government Act.	OMB

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
101	**OMB Memorandum 00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000)**	OMB Guidelines	Prohibits the use of persistent cookies to track an individual's activity on Internet; prohibition on use of "tracking technology" in general is picked up in OMB Memorandum 03-22, above.	Yes.	Federal Web site usage data.	OMB
102	**OMB Memorandum M-05-08, February 2005**	OMB Guidelines	Requests appointment of "senior agency officials for privacy" and lays out other privacy expectations.	Yes.	Personally identifiable information in possession of agency.	OMB
103	**DOJ—Law Enforcement Information Sharing Program (LEISP)**	DOJ Policy	National strategy developed by state/local law enforcement personnel to enhance intelligence-based policing.	Document referenced in compilation but not described—not further reviewed.	Law enforcement information.	G1a
104	**DHS Management Directive Number 11042.1, "Safeguarding Sensitive but Unclassified ("For Official Use Only") Information," January 6, 2005**	DHS Directive	DHS rules for FOUO information.	Yes—Requires FOUO designation for information exempt from disclosure under the Privacy Act or the disclosure of which could adversely affect a person's privacy.	DHS information.	G1a
105	**DHS Privacy Act Procedures, 6 CFR Part 5**	DHS Regulations	DHS Privacy Act regulations.	Yes.	DHS Privacy Act information.	G1a
106	**FBI Name Check Program**	Interagency Agreement	Interagency agreement to share information with the FBI.	Document referenced in compilation but not described—not further reviewed.	Document referenced in compilation but not described—not further reviewed.	G1a
107	**FinCEN MOU**	Interagency Agreement	Provides data related to financial crimes shared via U.S. Department of the Treasury.	Document referenced in compilation but not described—not further reviewed.	Financial data.	G1a

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
108	**Fingerprint Cards and Name Checks**	Interagency Agreement	Interagency agreement to share information with the FBI.	Document referenced in compilation but not described—not further reviewed.	Document referenced in compilation but not described—not further reviewed.	G1a
109	**Visa Processing MOU**	Interagency Agreement	Interagency agreement to share information with the FBI.	Document referenced in compilation but not described—not further reviewed.	Document referenced in compilation but not described—not further reviewed.	G1a

Page is intentionally left blank.

Appendix C
Policy Development Tool

Page is intentionally left blank.

Information Sharing Environment (ISE) Policy Development Tool

Background: The ISE Privacy Guidelines require federal agencies to develop and implement a written ISE privacy protection policy that sets forth agency mechanisms, policies, and procedures for implementing the ISE Privacy Guidelines.[7]

Purpose: The purpose of this tool is to provide federal agencies with a resource to utilize when developing their ISE privacy protection policy. This tool is associated with STAGE I, Step 2 and Step 3 of the Privacy and Civil Liberties Implementation Guide. It is designed to assist agencies in assessing existing policies and procedures compared to the ISE Privacy Guidelines requirements and, from that assessment, identify gaps in policy. Upon completion, the Development Tool should assist agencies in writing their ISE privacy protection policy by (1) having existing policies—references and text—that can be "pasted" into the new policy, (2) knowing what gaps in policy need to be filled, and (3) knowing what is necessary to meet a particular ISE Privacy Guidelines requirement, thereby helping the agency to write a new policy that meets the particular requirement.

Instructions:

- The first column identifies the ISE Privacy Guidelines requirement and required agency policy and procedure responsibilities, as specified in the Guidelines. The requirements are bolded to clearly identify what is required by agencies.

- The second column provides core policy and procedure elements that, if implemented by an agency, demonstrate compliance with the associated Guidelines requirement. If the column has an "N/A," there is no associated core element. Agencies should refer to Appendix D—Key Issues Guidance for additional guidance in complying with the associated core element.

- The third column is for agencies to cite to a document(s) in which the Guidelines requirement is fulfilled, in whole or in part, by preexisting agency policies and procedures. It is recommended that the policy and procedure language and reference be reproduced in this column to ensure a comprehensive and accurate ISE privacy protection policy. If the policy cited or set forth in this column wholly meets the ISE Privacy Guidelines requirements, then the next column should be blank.

- The last column is for agencies to "fill in" with new, revised, or additional policies and procedures that adhere to the corresponding ISE Privacy Guidelines requirement, if the agency does not have a preexisting agency policy in place.

- Once the Policy Development Tool is complete, transfer the information to Appendix E—ISE Privacy Policy Outline to produce the written ISE privacy protection policy. An agency should utilize its normal process for obtaining agency approval for the issuance of the policy.

[7]See ISE Privacy Guidelines, 12. Governance, d. ISE Privacy Protection Policy.

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements (See Key Issues Papers for additional detail and background information)	Existing Agency Policy • Document location/ reference • Suggest reproducing actual policy language	New Policy • Addresses gaps in policy protection
1. Background and Applicability			
1a. Background. The ISE Privacy Guidelines (Guidelines) implement requirements under the IRTPA and EO 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.	**N/A**		
1b. Applicability. The Guidelines apply to "protected information" as defined in Section 1(b) of the Guidelines.	**N/A**		
2. Compliance with Laws			
2a. General. In the development and use of the ISE, all agencies shall, without exception, **comply with the Constitution and all applicable laws and Executive Orders relating to protected information.**	**N/A**		
2b. Rules Assessment. Each agency shall **implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE**. Each agency shall **identify, document, and comply with any legal restrictions applicable to such information**. Each agency shall **adopt internal policies and procedures requiring it to:** **(i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and**	**N/A**		
(ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.			

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
2c. Changes. **If, as part of its rules assessment process, an agency:** **(i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall** as appropriate **develop policies and procedures to provide protections that address that issue;**	**N/A**		
(ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 of the Guidelines) **in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction;**			
(iii) identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 of the Guidelines)**, and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI).**			

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
3. Purpose Specification			
3. Purpose Specification. **(Share) Protected information through the ISE only if it is terrorism information, homeland security information, or law enforcement information** (as defined in Section 13 of the Guidelines). Each agency shall **adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected information available through the ISE is consistent with the authorized purpose of the ISE.**	**N/A**		
4. Identification of Protected Information to be Shared through the ISE*			
4a. Identification and Prior Review. In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance With Laws) and Section 3 (Purpose Specification) of the Guidelines, each agency shall **identify its data holdings that contain protected information to be shared through the ISE and** shall **put in place such mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to the Guidelines before it is made available to the ISE.**	**N/A**		

* See "Key Issue Guidance: Notice Mechanisms" (pp. B1–B9) for additional in-depth guidance regarding core elements in this section.

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
4b. Notice Mechanisms. Consistent with guidance and standards to be issued for the ISE, each agency shall **put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements.** **Specifically, such a mechanism will**, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements**, allow for ISE participants to determine whether:** **(i) the information pertains to a United States citizen or lawful permanent resident;**	Status of record subject(s): a. U.S. citizen b. Lawful permanent resident (LPR) c. Noncitizen or non-LPR protected by treaty or international agreement d. Undetermined		
(ii) the information is subject to specific information privacy or other similar restrictions on access, use, or disclosure and, if so, the nature of such restrictions; and	Restrictions on access, use, or disclosure: a. Nature of restriction b. Source of restriction		
(iii) there are limitations on the reliability or accuracy of the information.	Reliability and accuracy of information: a. Nature of source b. Confidence c. Data quality		

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
5. Data Quality*			
5a. Accuracy. Each agency shall **adopt and implement procedures**, as appropriate, **to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.**	• Protected information (PI) originating in the agency is as accurate, complete, and internally consistent as the agency requires for use in making determinations, given its authorities and mission. • PI is relevant and timely as appropriate for agency use, and when it becomes outdated or irrelevant for such agency use, it is updated, deleted, or not used in the ISE. • PI originating in the agency indicates to recipients any known limitations on its reliability or accuracy.		
5b. Notice of Errors. Each agency, consistent with its legal authorities and mission requirements, shall **ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official** (the ISE privacy officials are described in Section 12 of the Guidelines).	• Where feasible, written notice is given to the providing agency's ISE Privacy Official of specific PI that the receiving agency has determined is erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the subject may be affected.		

* See "Key Issue Guidance: Data Quality" (pp. C1–C12) for additional in-depth guidance regarding core elements in this section.

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
5c. Procedures. Each agency, consistent with its legal authorities and mission requirements, shall **adopt and implement policies and procedures with respect to the ISE requiring the agency to:** **(i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;**	• Information the agency has matched against or consolidated from multiple sources relates to the same individual.		
(ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and	• Alleged or identified errors or deficiencies in PI about which the agency is notified are investigated in a timely manner. • PI an agency investigation determines is erroneous or deficient for its purposes is corrected or deleted, or if not corrected or deleted, the agency refrains from sharing it through the ISE. • PI recipients, to the extent they can be identified, are notified of alleged or identified errors or deficiencies in the providing agency's information that has been disseminated in the ISE, including incorrect mergers/matches/ insertions of information.		

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
(iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.			
	6. Data Security*		
6. Data Security. Each agency shall **use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.**	Non-National Security Systems: a. Security categorization standards (low-, moderate-, and high-impact). b. Minimum security requirements (keyed to system impact category). c. Implementation of controls (keyed to minimum security requirements. National Security Systems: a. Defense Information Assurance Certification/ Accreditation Process. b. National Information Assurance Certification/ Accreditation Process. c. Director of CIA 6/3. d. National Information Assurance Policy No. 11.		

* See "Key Issues Guidance: Data Security" (pp. D1–D9) for additional guidance regarding core elements in this section.

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
7. Accountability, Enforcement and Audit*			
7a. Procedures. Each agency shall **modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to:** **(i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;**	Policy framework that addresses: a. Training of personnel authorized to handle PI in the ISE. b. Reporting violations of agency privacy. protection policies c. Investigating indentified/reported violations of agency privacy protection policies. d. Responding to identified/reported violations of agency privacy protection policies. e. Cooperating with audits and reviews by appropriate internal and external audit and oversight authorities. f. Measures ensuring that the agency ISE privacy official receives copies of all reports/notices regarding alleged errors in PI content that the agency has disseminated in the ISE.		

* See "Key Issues Guidance: Accountability, Enforcement, and Audit" (pp. E1–E10) for additional guidance regarding core elements in this section.

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
(ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, **for reporting violations of agency privacy protection policies;**			
(iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and			
(iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.			
7b. Audit. Each agency shall **implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with the Guidelines in the development and use of the ISE.**	Program review framework/ inspection process for examining compliance with the ISE Privacy Guidelines in the following areas: a. Compliance with laws b. Purpose limitation c. Identification of PI d. Notice mechanisms e. Data quality f. Data security g. Accountability, enforcement, and audit h. Redress i. Execution, training, and technology j. Public awareness of agency policies and procedures		

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
8. Redress*			
8. Redress. To the extent consistent with its legal authorities and mission requirements, each agency shall, **with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.**	• Describe existing procedures for addressing complaints arising under the Constitution, Privacy Act, or other statutes. Describe policies, procedures, and personnel dedicated to addressing complaints resulting from the agency's use of PI originating from another agency. • Describe policies, procedures, and personnel dedicated to assisting other agencies in addressing matters involving PI an agency provided through the ISE. • Describe procedures (as needed) developed and implemented for addressing complaints regarding PI in the ISE that are not otherwise covered by existing procedures.		
9. Execution, Training, and Technology			
9a. Execution. **The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs.**	**N/A**		

* See "Key Issues Guidance: Redress" (pp. A1–A8) for additional guidance regarding core elements in this section.

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
9b. Training. Each agency shall **develop an ongoing training program in the implementation of the Guidelines, and provide such training to agency personnel participating in the development and use of the ISE.**	**N/A**		
9c. Technology. Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall **consider and implement**, as appropriate, **privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.**	**N/A**		
10. Awareness			
10. Awareness. Each agency shall take steps to **facilitate appropriate public awareness of its policies and procedures for implementing the Guidelines.**	**N/A**		
11. Non-Federal Entities			
11. Non-Federal Entities. Consistent with any standards and procedures that may be issued to govern participation in the ISE by State, tribal, and local governments and private sector entities, the agencies and the PM-ISE will **work with non-Federal entities seeking to access protected information through the ISE to ensure that such non-Federal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the Guidelines.**	**N/A**		

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
12. Governance			
12a. ISE Privacy Officials. **Each agency's senior official with overall agency-wide responsibility for information privacy issues** (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005), **shall directly oversee the agency's implementation of and compliance with the Guidelines** (the "ISE privacy official"). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency. The ISE privacy official role may be delegated to separate components within an agency, such that there could be multiple ISE privacy officials within one executive department. **The ISE privacy official shall be responsible for ensuring that (i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these Guidelines, and (ii) changes are made as necessary. The ISE privacy official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE.** Such authority should be exercised in coordination with the agency's senior ISE official.	**N/A**		
12b. ISE Privacy Guidelines Committee. All agencies will **abide by these Guidelines in their participation in the ISE.**	**N/A**		
12d. ISE Privacy Protection Policy. Each agency shall **develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines.** Agencies should **consult with the ISE Privacy Guidelines Committee as appropriate in the development and implementation of such policy.**	**N/A**		

ISE Privacy Guidelines: Agency Policy and Procedure Responsibility	Core Policy and Procedure Elements	Existing Agency Policy	New Policy
13. Definitions			
13. Definitions. This section defines the terms "protected information," "terrorism information," "homeland security information," and "law enforcement information."	**N/A**		

Appendix D
Key Issues Guidance

Page intentionally left blank.

Table of Contents

Guidance Papers Outline

Background

- The guidance papers in these sections provide additional in-depth guidance on selected areas of the ISE Privacy Guidelines. They were developed through extensive review and coordination by interagency working groups consisting of Federal privacy and civil liberties officials and attorneys and were reviewed and approved by the ISE Privacy Guidelines Committee and the Information Sharing Council.

Purpose

- The purpose of the guidance papers is to provide guidance in interpreting certain ISE Privacy Guidelines requirements and to outline possible methods or "best practices" to assist agencies in implementing those requirements. These guidance papers do not create new or modify existing policy.

Policy Guidance

- The **policy guidance section** identifies the core, or basic, elements that an agency must address in order to comply with key requirements of the ISE Privacy Guidelines that are the subject of a guidance paper. It also identifies optional suggested elements that contribute to the formulation of an exemplary privacy, civil rights, and civil liberties protection policy.

Background and Commentary

- The **background and commentary section** provides additional background information on the subject area, including its relationship to the Federal Information Processing Standards (FIPS), the background rationale for the ISE Privacy Guidelines provision, and a discussion of some of the key issues in that subject area. This section also cites resource documents and provides appropriate links.

Resources and Tools

- The **resources and tools section** provides helpful checklists, guidelines, documents, and best-practices information designed to assist agencies in formulating and implementing sound privacy, civil rights, and civil liberties policies.

Note on ISE Privacy and Civil Liberties Implementation Guidance

The ISE Privacy Guidelines contain references to requirements that agencies put in place—policies and procedures—as appropriate and consistent with their legal authorities and missions. Such references are not intended to imply that agencies are required to adopt policies and procedures that would impair the agencies' abilities to exercise their statutory authorities and responsibilities, including the ability to claim exemptions under the Privacy Act of 1974 or to comply with the requirements of any other law, or that would negatively affect their position in

litigation or administrative proceedings. As noted in Section 13 (d)(iv) of the ISE Privacy Guidelines: "These Guidelines…are intended only to improve the management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person."

REDRESS

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 8, provide that:

> To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

As the ISE is developed, individuals may experience circumstances that lead them to question whether protected information (PI)[8] about them might be erroneous, improperly collected, or inappropriately shared or used as part of the ISE, and they may wish to have the situation corrected. Because individuals will not always know the source of the information, complaints most likely will be lodged with the Federal agency which the complainant believes is responsible, rather than with the agency which originated the information and made it available in the ISE. Accordingly, in implementing Section 8, Federal agencies should review their existing complaint-handling procedures to determine whether they accommodate issues pertaining to PI shared in the ISE. The objective is to ensure that internal and external processes exist for handling complaints involving information originating with another agency and for assisting other agencies in receipt of complaints involving information for which an agency is the source. As needed, agencies shall establish procedures appropriate for addressing complaints arising from the sharing of PI in the ISE but only to the extent such procedures do not conflict with legal authorities and mission requirements.

[8] Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

Redress has been recognized as a useful mechanism to improving data integrity by ensuring data is current, complete, and accurate. However, as noted, this guidance is intended only to assist agencies in implementing the ISE Privacy Guidelines—it neither affects any existing agency policy or Privacy Act exemptions, nor is it intended to create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, entities, officers, employees, or agencies or any other person.

Agency ISE redress procedures should address the following core elements:

Core Elements

1. A description of the existing procedures for addressing complaints arising under the Constitution (including nonprivacy civil rights and civil liberties), Privacy Act, or other statutes (including civil rights and civil liberties statutes).

2. A description of policies, procedures, and personnel dedicated toward addressing complaints resulting from the agency's use of PI originating from another agency (if any).

3. A description of policies, procedures, and personnel dedicated toward assisting other agencies to address matters involving PI an agency provided through the ISE (if any).

4. A description of procedures (as needed) developed and implemented for addressing complaints regarding PI in the ISE that are not otherwise covered by existing procedures (see 2 and 3 above).

Additional Considerations

1. Identify record-keeping practices and objectives (i.e., improving processes).

2. Develop and disseminate (via public affairs office, privacy office, civil liberties/civil rights office, Equal Employment Opportunity [EEO] office, Web page, and other) information regarding agency policy/process for addressing PI/ISE-related complaints.

BACKGROUND AND COMMENTARY[9]

Section 8 of the ISE Privacy Guidelines states the following with respect to redress:

> Redress. To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

The persons covered by these Guidelines are described in paragraph 1(b) as follows:

> *Applicability*. These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

The ISE Privacy Guidelines require each agency participating in the ISE, consistent with its legal authorities and mission requirements, to provide "redress"; i.e., a procedure for addressing complaints relating to PI in the ISE. The ISE Privacy Guidelines contemplate that agencies will afford redress with respect to issues involving information privacy, as well as alleged infringements of civil rights, civil liberties, and other legal rights protected by law. Therefore, as appropriate, agency procedures would permit persons to use the agency's existing complaint/review procedures or any supplementary procedures developed for the ISE to address such complaints as alleged racial, ethnic, or religious profiling or retention in the ISE of information that has been expunged or determined to have been illegally collected.

Many participating ISE agencies already have in place procedures for handling all manner of complaints, including privacy, civil rights, and civil liberties unrelated to the ISE.[10] The redress procedures contemplated by the ISE Privacy Guidelines are limited to situations involving complaints that the agency determines implicate PI in the ISE (although not necessarily under the control of the agency receiving the complaint). The ISE policy requirement to implement

[9] The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. It is not a binding interpretation of law, regulation, or policy.

[10] H.R. 1, Title VIII, Section 803, amends Section 1062 of the IRTPA to require that named Federal agencies "(3) ensure that such department, agency, or element has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties."

internal complaint-handling procedures for ISE-related issues neither alters agency rules regarding record access or other rights nor requires agencies to either acknowledge the existence of records or inform complainants of case status or resolution where no such right currently exists. As is true under existing processes, many information privacy, Privacy Act, or civil rights and civil liberties complaints identified as involving PI in the ISE will not result in the complainant being informed of measures the agency takes to investigate a complaint, rectify an alleged error, or remedy an issue.

Because individuals and entities covered by these guidelines often may not recognize that there is any relationship between the complaint and the ISE, agencies must establish, as part of their procedure to address complaints, a process that will identify those complaints that are related to PI in the ISE. These complaints generally will be received through existing agency avenues of redress (e.g., Privacy Act requests, existing agency civil rights and civil liberties processes). Once an agency determines that a complaint, which may be received as a general complaint, concerns PI originating with the agency or obtained through the ISE, the principles of ISE redress require the agency to coordinate with all involved agencies to investigate and correct (or remove) any identified information deficiencies.

Agencies must review their existing complaint policies and procedures to ensure that processes exist to identify complaints involving PI in the ISE and to bring them to the attention of the agency's ISE Privacy Official or designee. (See Data Quality issue paper addressing the ISE Privacy Official's responsibility for data quality.) Thus, the ISE Privacy Guidelines' focus is on providing a process by which complaints implicating PI in the ISE are identified and addressed.

The ISE Privacy Guidelines protect the information privacy and other legal rights of United States citizens and lawful permanent residents and, for the intelligence community, United States persons. However, these categories of PI may be expanded to include other information that the United States government expressly determines by Executive Order, international agreement, or other similar instrument shall be covered by the ISE Privacy Guidelines. Indeed, many agencies share PI pursuant to international agreements that allow foreign nationals access to review procedures (e.g., the agreement with the European Union [EU] involving Passenger Name Records). Where a complaint/review process is required by international agreement, special procedures may be employed for foreign nationals (to the extent that such details are not spelled out in the agreement).

The following is a list of authorities that may assist ISE participants in developing their redress policies and procedures for PI in the ISE:

Executive Orders

Executive Order 12333, *United States Intelligence Activities*, December 4, 1981, as amended. http://www.whitehouse.gov/news/releases/2004/08/20040827-6.html

Executive Order 13353, *Establishing the President's Board on Safeguarding Americans' Civil Liberties*, August 27, 2004. http://www.whitehouse.gov/news/releases/2004/08/20040827-3.html

Executive Order 13356, *Strengthening the Sharing of Terrorism Information to Protect Americans*, August 27, 2004. http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html

Executive Order 13311, *Homeland Security Information Sharing*, July 29, 2003. http://a257.g.akamaitech.net/7/257/2422/20apr20040800/edocket.access.gpo.gov/cfr_2004/janqtr/pdf/3CFR13311.pdf

Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October, 25, 2005. http://www.ise.gov/docs/guidance/eo13388.pdf

Policy Guidance and Standards

OMB *Privacy Act Implementation, Guidelines, and Responsibilities* ("OMB Guidelines") 40 *Federal Register* 28,948 and 28,965 (July 9, 1975). http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf

U.S. Department of Homeland Security (DHS) Privacy Policy Guidance Memorandum, 2007-1, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information.* http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf

Memorandum of Understanding on Terrorist Watchlist Redress Procedures. http://www.fbi.gov/terrorinfo/counterrorism/redress_mou.pdf

Commentators

Paul Rosenzweig and Jeff Jonas, *Correcting False Positives: Redress and the Watch List Conundrum*, June 17, 2005 (Heritage Foundation).
http://www.heritage.org/Research/HomelandDefense/upload/79671_1.pdf

Markle Foundation, *Implementing a Trusted Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability*, February 2006.
http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf

Center for Democracy and Technology, *Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information*, February 2, 2007.
http://www.cdt.org/security/20070205iseanalysis.pdf

Web Sites—Examples of Federal Agency Redress Policies

DHS Traveler Redress Inquiry Program (DHS TRIP)—single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs—such as airports and train stations—or crossing U.S. borders.
http://www.tsa.gov/travelers/customer/redress/index.shtm

Federal Bureau of Investigation (FBI), Terrorist Screening Center, Redress Procedure.
http://www.fbi.gov/terrorinfo/counterrorism/redress.htm

RESOURCES AND TOOLS

In developing their ISE redress procedures, agencies may wish to use the following checklist and consider the following specific matters:

Core Elements

1. Describe existing redress and complaint procedures:
   a. Identify all agency-internal avenues for handling complaints (i.e., for all manner of complaints cognizable under statute or regulation or policy):
      (i) Civil Rights/Civil Liberties
      (ii) Privacy Act
      (iii) EEO
      (iv) OIG
      (v) Ombudsman
      (vi) Other
   b. Identify all interagency complaint initiatives that your agency supports:
      (i) DHS Traveler Redress Inquiry Program (TRIP)
      (ii) TSC Terrorist Watchlist Redress Process (MOU)
      (iii) Other

2. Describe policies, procedures, and resources for identifying and addressing PI/ISE-related complaints resulting from the agency's use of PI originating elsewhere.

3. Describe policies, procedures, and resources for assisting other ISE agencies to address complaints arising from their use of PI originating with your agency.

4. Establish procedures (as needed) for addressing privacy or civil liberties complaints relating to PI in the ISE and not otherwise subject to existing procedures:
   a. Provide identity and contact information for agency office of the ISE Privacy Official—e.g., a mailing address (USPS or e-mail) and/or a telephone number(s) of responsible staff.
   b. Ensure that all agency complaint-handling components are familiar with the ISE and understand when a complaint received implicates PI subject to ISE redress.
      - Establish process/information to assist non-ISE-complaints staff in identifying when a complaint involves PI in the ISE.
   c. Establish appropriate liaison with ISE participants from which data will likely originate to facilitate complaint investigation processes.
      - Provide a point of contact and responsible official to ensure appropriate reciprocal support to complaint recipients.

d. Explain processes for coordinating investigation of PI/ISE-related complaints both internally and externally.
e. Develop tools required under the Privacy Act for administering the PI/ISE complaint "program," such as:
   (i) Establish or identify an appropriate system of records to maintain complaints and related information.
   (ii) Ensure that the system of records notice associated with the redress system contains a routine use to allow disclosure of complaint and personally identifiable information to other agencies and organizations to the extent necessary to investigate and address the complaint.
   (iii) Identify records retention obligations.
f. Develop procedures for responding to identified ISE-related complaints.
   (i) Leverage existing agency procedures for establishing/verifying identity or status where appropriate.
   (ii) Develop protocol for acknowledging complaint.
      (a) May wish to articulate scope of redress available:
         - Investigation of alleged errors.
         - Correction of alleged errors/removal of data.
         - Notification of correction to originator and downstream recipients of record.
      (b) May wish to articulate limits of redress afforded:
         - No remedy for underlying injury.
         - No right of action.
         - Particular forms of redress (e.g., right of access to records, notice of resolution of complaint, explanation of investigatory process) may be unavailable given national security, law enforcement equities, or other security considerations relating to terrorism.

Additional Considerations

1. Identify record-keeping objectives intended to enhance ISE processes:
   a. Record PI/ISE complaints received and disposition.
   b. Maintain unresolved PI/ISE complaints.
   c. Examine policy/process changes (if any) needed for PI/ISE review process.

2. Develop outreach/public awareness materials regarding agency PI/ISE redress framework:
   a. Explain process for identifying ISE-related complaints.
   b. Explain processes for investigating and addressing complaints, internally and externally.
   c. Explain "redress" available; i.e., data quality activities.

NOTICE MECHANISMS

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 4(b), provide the following Notice Mechanisms requirement:

> b. *Notice Mechanisms.* Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:
>
> (i) The information pertains to a United States citizen or lawful permanent resident;
> (ii) The information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and
> (iii) There are limitations on the reliability or accuracy of the information.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

Section 4(b) of the ISE Privacy Guidelines recognizes that enabling agencies to determine important characteristics of protected information (PI)[11] available in the ISE— such as the status of an individual; any restrictions on access, use, or disclosure of PI; and any limitations on its reliability and accuracy—will promote a trusted information sharing environment as recipient agencies are made aware of these aspects of PI and can determine whether access to, use of, and further disclosure of the data are consistent with agency missions and applicable legal requirements. Providing restrictions and limitations on information as part of a record, data set,

[11] Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

or record system will also serve to mitigate potential risks arising from information sharing activities for all agencies participating in the ISE.

This ISE Privacy Guidelines Notice Mechanisms Guidance comports with the proposed marking of Controlled Unclassified Information (CUI) recommended under the framework described in the proposed Presidential Guideline 3 report, *Standardized Procedures for Sensitive But Unclassified (SBU) Information* (issuance pending). While the proposed CUI framework under Guideline 3 contemplates a limited set of approved "markings" reflecting handling and dissemination requirements, the elements of notice set forth above from the ISE Privacy Guidelines relating to the status of an individual and reliability and accuracy of the information are intended to reflect the nature and quality of the information itself and to be incorporated within an individual record, data set, or record system. These notice mechanisms for privacy requirements are not a handling or dissemination requirement. This guidance should be read in conjunction with the proposed CUI framework and should not be read to foreclose the possibility that notice of "specific information privacy or other similar restrictions on access, use, or disclosure" may be addressed through a CUI marking in the future.

To incorporate appropriate notice, agencies creating reports or disseminating products containing PI in the ISE may continue their customary practices in providing information about their individual records, data sets, or record systems that assists in determining whether the information pertains to an individual's status, any restrictions on access, use, or disclosure, and any limitation on reliability or accuracy of the information. Agencies may use, among other methods, a simple cover sheet to flag such issues or, for electronic information, may use banners, legends, or full-screen notices signaling the general character of and restrictions on access, use, or disclosure of records in the data set or record system.

As may be reasonable and consistent with agencies' legal authorities and mission requirements, agencies engaging in the ISE should consider adopting mechanisms to provide notice of each of the following core elements of information:

Core Elements

1. Status of record subject(s):
   a. U.S. citizen
   b. Lawful permanent resident (LPR)

c. Noncitizen or non-LPR protected by treaty or international agreement
d. Undetermined

2. Restrictions on access, use, or disclosure:
   a. Nature of restriction
   b. Source of restriction

3. Reliability and accuracy of information:
   a. Nature of the source—indicating the origin of the information
   b. Confidence—source reliability and content validity
   c. Data quality—inconsistencies or other accuracy concerns based on:
      (i) Notice received from previous recipients of the data
      (ii) Disagreements about accuracy received from the record subject or other person negatively impacted by the record
      (iii) Evaluation of data in context with other existing records (See Data Quality Guidance)
      (iv) Results of compliance reviews or external audits

Additional Considerations

1. Basic source and point-of-contact information
   a. Originating department, component, or office
   b. Agency system from which information is disseminated
   c. Date of collection/date last used to make a determination about an individual, if applicable
   d. Title/contact for questions about the information or access request, if appropriate

2. Date of last data accuracy review conducted in accordance with agency policy and procedure (see Data Quality Guidance)

BACKGROUND AND COMMENTARY[12]

Background and Purpose

In the ISE, the information that is accessed or disseminated (disclosed) comes from numerous sources and often includes (1) protected information (PI), (2) information to which information privacy or other legal protections have been extended, and (3) information for which the status is undetermined or is not privacy-protected. Consequently, ISE participants may be bound by various legal requirements that govern access, use, and disclosure. The quality of the information in the ISE will also vary in reliability and accuracy. Therefore, as information is disclosed in the ISE, the ISE Privacy Guidelines require agencies to implement mechanisms to indicate to recipients whether information disclosed pertains to a U.S. citizen or lawful permanent resident; whether there are legal requirements that protect information privacy or other legal rights of the subject or restrict access, use, or disclosure of the information; and whether the source or providing agency considers the information to be of limited reliability or accuracy.

The purpose of this document is not to examine the range of notice mechanisms technology or to list all of the specific restrictions that might apply with respect to access, use, and disclosure of information in the ISE. Instead, this document focuses on the information about PI that could be included in individual records, data sets, or record systems that may be shared in the ISE.

In the ISE, information regarding PI; any specific information privacy; or other similar restrictions on access, use, or disclosure, and limitations on the reliability or accuracy of the information may be incorporated in a record, data set, or record system before it flows from its originating source or other provider to its end user.

Nature of the Information—Identify Status of Individuals

The status of data subjects may determine the degree of protection, if any, that they will receive in the ISE. Therefore, notice regarding limitations on access, use, or dissemination will necessarily begin with a determination of whether the information applies to U.S. citizens, lawful permanent residents (LPRs), or non-U.S. citizens who are not LPRs but who may, nevertheless, receive protection in the ISE. Suggested categories include:

[12]The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. This section neither establishes policy under the ISE nor is binding on any department or agency participating in the ISE. It is not a binding interpretation of law, regulation, or policy.

1. U.S. citizen[13]
2. Lawful permanent resident[14]
3. Non-U.S. citizen or non-LPR protected by treaty or other international agreement[15]
4. Undetermined

Limitations on Access, Use, or Disclosure—Identify Restrictions on Access, Use, or Disclosure:

Identify any legal restrictions on access, use, or disclosure of PI and the nature of the restrictions. There are numerous statutory and regulatory limitations that pertain to different types of information that may be shared in the ISE.[16]

Limitations on Reliability and Accuracy (Validity)—Identify Confidence Limitations:

There are existing efforts in some law enforcement and intelligence agencies at the Federal, state, local, and tribal levels to provide law enforcement information in a way that conveys to the recipient the originating agency's level of confidence in the information; i.e., its assessment of the information's (source) reliability and (content) validity. The U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative's *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*[17] (hereinafter "Justice PCRCL Policy Templates") recommends that the following assessment typology be incorporated into the body of the record as appropriate to the nature of the information and the level of protection required:

[13] U.S. citizenship can be obtained in one of two ways: (1) by birth, either within the territory of the United States or to U.S. citizen parents, or (2) by naturalization. http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=96719c7755cb9010VgnVCM10000045f3d6a1RCRD&vgnextchannel=96719c7755cb9010VgnVCM10000045f3d6a1RCRD. See also United States Immigration and Nationality Act, Title 8 of the U.S. Code (8 U.S.C.).

[14] According to United States Citizenship and Immigration Services (USCIS), "[A] lawful permanent resident is a foreign national who has been granted the privilege of permanently living and working in the United States." http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=0775667706f7d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=4f719c7755cb9010VgnVCM10000045f3d6a1RCRD

[15] Individuals who are not U.S. citizens or lawful permanent residents may receive certain protections in the ISE under the terms of an international agreement (e.g., the agreement with the EU involving Passenger Name Records).

[16] See "2006 Interagency Assessment of Federal Privacy and Civil Liberties Policies that Impact Information Sharing," Privacy and Civil Liberties Implementation Manual, Tab V, Section D2.

[17] DOJ's Global Justice Information Sharing Initiative, *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*, February 2008, at p. 20. http://www.it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf

1. Nature of the Source. Nature of the source simply identifies the origin of the information.
    a. Anonymous tip
    b. Informant
    c. Interview or written statement (subject, victim, witness, etc.)
    d. Public records (space should be provided for identifying the government system from which the information was derived because that may bear on its reliability)
    e. Private sector (notice should be given if the information was collected from a data aggregator or broker)
    f. Other (please specify)

2. Source Reliability. Source reliability addresses the consistency of the content validity of information obtained from a particular source over time.
    a. Reliable—the reliability of the source is trusted or has been well tested in the past
    b. Usually Reliable—the source can usually be relied upon
    c. Unreliable—the reliability of the source has been sporadic in the past
    d. Unknown—the reliability of the source cannot be judged

3. Content Validity. Information content deals with the accuracy or truth of the information independent of its source (i.e., even generally unreliable sources can sometimes provide reliable information).
    a. Confirmed—information has been corroborated by an investigator or
    b. Another reliable source
    c. Probable—the information is consistent with past accounts
    d. Doubtful—the information is inconsistent with past accounts
    e. Cannot be judged—the information cannot be judged

This type of assessment allows investigators to determine the extent to which they may rely on the information and the extent to which verification from other sources will be required.

The ISE Data Quality Guidance provided at Divider VI, Tab C, of the Privacy and Civil Liberties Implementation Manual (PM-ISE 2007) suggests additional considerations regarding notice of information accuracy, relevancy, timeliness, and completeness; e.g., based on specific challenges to accuracy of the data received from recipient entities or record subjects or unresolved concerns arising from internal review.

Identify Basic Information

To the extent feasible and consistent with agency legal authorities and mission requirements, agencies should consider developing or expanding individual records, data sets, or record systems to include information about the provider of the data. The following elements of information would facilitate follow-up or inquiry:

1. The name of the originating department, component, or subcomponent.
2. The name of the agency system from which the information is disseminated.
3. The date the information was collected and the date it was last used to make a determination about an individual.
4. The title and contact information for the person to whom questions regarding the information should be directed.

The following is a list of authorities that may assist ISE participants in developing their notice mechanisms policies and procedures for PI in the ISE:

Policy Guidance and Directives

Presidential Guideline 3 report, *Standardized Procedures for Sensitive But Unclassified (SBU) Information* (issue pending), Privacy and Civil Liberties Implementation Manual (PM-ISE, 2007) (see also www.ise.gov).

ISE Data Quality Guidelines, Divider VI, Tab C, Privacy and Civil Liberties Implementation Manual (PM-ISE, 2007) (see also www.ise.gov).

DHS Privacy Office Privacy Policy Guidance Memorandum Number 2007-1, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, January 19, 2007.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

U.S. Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, at p. 23.
http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf (discussing redress issues at the Terrorist Screening Center).

Web Sites

United States Citizenship and Immigration Services Web site:
http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=0775667706f7d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=4f719c7755cb9010VgnVCM10000045f3d6a1RCRD (defining requirements for U.S. citizenship) and

http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=8b76194d3e88d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=4f719c7755cb9010VgnVCM10000045f3d6a1RCRD (defining requirements for becoming a lawful permanent resident).

RESOURCES AND TOOLS

RESERVED

DATA QUALITY

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 5, provide the following Data Quality requirement:

a. *Accuracy*. Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.

b. *Notice of Errors.* Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official (the ISE privacy officials are described in Section 12 below).

c. *Procedures.* Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:

(i) Take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;
(ii) Investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and
(iii) Retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

Section 5 of the ISE Privacy Guidelines requires each agency participating in the ISE to adopt and implement procedures, as appropriate, regarding quality assurance measures to facilitate the prevention, identification, and correction of any errors in protected information (PI)[18] in order to ensure the information is accurate and has not erroneously been shared through the ISE. The full value of the ISE may be realized only if PI shared in the ISE is accurate, relevant, timely, and complete to the extent the providing and receiving agencies' missions require and any information identified as erroneous or deficient is corrected, updated, deleted, or not used, as administratively and technically feasible.[19]

Consistent with legal authorities and mission requirements, agency policies and procedures should address the following core data quality elements for information shared through the ISE:

Core Elements

1. PI originating in the agency is as accurate, complete, and internally consistent as the agency requires for use in making determinations, given its authorities and mission.

2. PI is relevant and timely as appropriate for agency use, and when it becomes outdated or irrelevant for such agency use, it is updated, deleted, or not used in the ISE.

3. PI originating in the agency indicates to recipients any known limitations on its reliability or accuracy (see also Notice Mechanisms Guidance).

[18] Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

[19] Erroneous or deficient information does not include information for which the reliability or validity may not be fully established. These elements of confidence in the information are the subject of Notice Mechanisms Guidance implementing Section 4(b) of the ISE Privacy Guidelines.

4. Where feasible, written notice[20] is given to the providing agency's ISE Privacy Official of specific PI that the receiving agency has determined is erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the subject may be affected.

5. Alleged or identified errors or deficiencies in PI about which the agency is notified are investigated in a timely manner.

6. PI an agency investigation determines is erroneous or deficient for its purposes is corrected or deleted, or if not corrected or deleted, the agency refrains from sharing it through the ISE.

7. PI recipients, to the extent they can be identified, are notified of alleged or identified errors or deficiencies in the providing agency's information that has been disseminated in the ISE, including incorrect mergers/matches/insertions of information.

8. Information the agency has matched against or consolidated from multiple sources relates to the same individual.

Additional Considerations

1. The agency maintains a record/accounting of data corrections/ additions provided and/or received.

2. The agency, in addition to providing written notice to the providing agency under Core Element 4 above, provides written notice to the originating (acquiring) agency where such agency is known and is not the providing agency.

[20] Written notice could include any form of nonverbal communication (such as e-mail or formal letter) that is capable of being retained as an official agency record. It is in the agency's discretion to determine who will be authorized to provide written notice to the providing agency and in what form.

BACKGROUND AND COMMENTARY[21]

The core principles for protecting privacy and civil liberties in the ISE require Federal agencies, consistent with agency legal authorities and mission requirements, to "[e]stablish data quality, accuracy, and retention procedures" that reflect basic privacy protections and best practices. The principles established in Section 5, Data Quality, of the ISE Privacy Guidelines, incorporate and build upon the data quality requirements of the Privacy Act of 1974.

The ISE Privacy Guidelines contemplate that Federal agencies will comply with both the Guidelines and all applicable Privacy Act requirements for all information in the ISE. This will require agencies to review their existing data quality policies and procedures and, where necessary, develop new policies and procedures applicable to ISE information that meet each of the requirements for accuracy, notice, information merger protection, investigation of alleged errors and deficiencies, and retention of information that are set forth in Section 5.

Section 8 of the ISE Privacy Guidelines, Redress, requires a procedure for identifying complaints involving PI in the ISE and for bringing them to the attention of the ISE Privacy Official or designee. This individual should be enabled, through the agency's Section 5 policies and procedures, to provide the redress contemplated under Section 8 and the Redress Policy Guidance, thereby furthering the agency's interest in limiting dissemination and maintenance of information in the ISE to information that is accurate, timely, relevant, and complete.

In the Federal government, there are two primary statutes that impose data quality requirements on Federal agencies: (1) the Privacy Act of 1974, P.L. 93-579, as amended, and (2) the Information Quality Act, Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001, P.L. 106-554 (codified at 44 U.S.C. §§ 3504(d)(1) and 3516)).[22]

[21] The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. It is not a binding interpretation of law, regulation, or policy.

[22] The Information Quality Act (IQA) requires Federal agencies subject to the Paperwork Reduction Act (44 U.S.C. § 3502(1)) to issue guidelines ensuring and maximizing the quality, objectivity, utility, and integrity of information including statistical information disseminated by the agency. The OMB Guidelines implementing the IQA (67 *Federal Register* 8452, February 22, 2002) define the term *dissemination* to mean "agency initiated or sponsored distribution of information to the public." Public dissemination includes posting information on government Web sites and in government manuals that are distributed to the public. However, per the OMB Guidelines, "Dissemination does not include distribution limited to government employees." Consequently, the IQA does not apply to records containing information about individuals that Federal agencies may share only internally or between agencies.

Data Quality Related Provisions of the Privacy Act of 1974

The Privacy Act can generally be characterized as an omnibus "code of fair information practices"[23] for the collection, maintenance, use, and dissemination of information about individuals by Federal agencies. The Privacy Act's protections apply to "individuals," which the act defines as U.S. citizens and lawful permanent residents (LPRs).[24]

The majority of the Privacy Act's provisions are limited to "records" (in paper or electronic form) that are in a "system of records" maintained by a Federal agency. In order to qualify as a "record" under the Privacy Act, the item, collection, or grouping of information must contain an identifying particular assigned to the individual (name, social security number, employee number, finger- or voiceprint, photograph, etc.) and be "about" the individual (i.e., include some descriptive item of information about the individual,[25] such as the individual's education, medical history, employment history, home address, or even any information provided by the system name alone; e.g., "Quarantined Persons"). Furthermore, the "record" must be maintained in a "system of records," which the Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[26]

Federal agencies that maintain systems of records must comply with the Privacy Act's data quality requirements. For example, unless a system of records is exempt (see below), Subsection (e)(5) of the Privacy Act requires that an agency "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[27] Accuracy, timeliness, relevance, and completeness are all elements of data quality. In addition, Subsection (e)(1) requires that an agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President."[28] Subsection (d) of the Privacy Act requires agencies to allow individuals to access information pertaining to them that is maintained in a system of records and to request that the agency amend a record if the individual believes the information is not accurate, relevant, timely, or complete. If the agency refuses to amend the record in accordance with the request, administrative and

---

[23] In 1972, a U.S. Department of Health, Education, and Welfare advisory committee proposed a "Code of Fair Information Practices." These practices formed the basis for the Privacy Act of 1974, and these "Fair Information Practices" are embodied as principles in the Privacy Act, as well as in a number of subsequent codes related to information collection, security, and privacy.

[24] In some circumstances, agencies may also provide certain Privacy Act protections to non-U.S. citizens and LPRs under the terms of an international agreement or as a matter of policy (see, for example, the agreement with the EU involving Passenger Name Records and DHS Privacy Policy Guidance Memorandum Number 2007-1 *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, January 19, 2007).

[25] OMB Guidelines, 40 *Federal Register* 28,948, 28,951-2 (July 9, 1975).

[26] 5 U.S.C. § 552a(a)(5)

[27] 5 U.S.C. § 552a(e)(5).

[28] 5 U.S.C. § 552a(e)(1).

judicial remedies are provided. Subsections (j) and (k), however, allow agencies to exempt certain records from specified provisions of the act, including Subsections (d), (e)(1), and (e)(5).

In enacting the Privacy Act, Congress recognized that the application of all of the act's requirements to certain categories of records could have undesirable and often unacceptable effects upon certain agencies in the conduct of necessary public business, particularly law enforcement[29] and national security agencies.[30] Consequently, Congress specifically authorized agencies to exempt particular systems of records from certain provisions of the Privacy Act. Nonetheless, no system of records is automatically exempt from any provision of the act. The agency that maintains a system must determine whether the system may be exempted and then promulgate a rule subject to the requirements of general notice and public comment as required by the Administrative Procedure Act, 5 U.S.C. § 551, 553 (1994). The rule must include the specific provisions from which the system is proposed to be exempted and specific reasons why the agency considers the exemption necessary.

[29]From OMB Privacy Act Implementation, Guidelines and Responsibilities [hereinafter OMB Privacy Act Guidelines], 40 *Federal Register* 28,948, 28,972 (July 9,1975), concerning provisions to exempt certain law enforcement records:

> This provision allows agency heads to exempt a system of records compiled in the course of an investigation of an alleged or suspected violation of civil laws, including violations of the Uniform Code of Military Justice and associated regulations, except to the extent that the system is more broadly exempt under the provision covering records maintained by an agency whose principal function pertains to the enforcement of criminal laws (subsection (j)(2)) . This exemption was drafted because '[i]ndividual access to certain law enforcement files could impair investigations, particularly those which involve complex and continuing patterns of behavior. It would alert subjects of investigations that their activities are being scrutinized, and thus allow them time to take measures to prevent detection of illegal action or escape prosecution.' (House Report 93-1416, p. 19)

[30]From OMB Privacy Act Guidelines, 40 *Federal Register* at 28,972, concerning provisions to exempt certain national security records:

> Useful guidance in the application of this provision is found in the Senate Committee report discussion of a similar provision on classified materials. 'The potential for serious damage to the national defense or foreign policy could arise if the notice describing any information system included categories or sources of information … or provided individuals access to files maintained about them…. The Committee does not by [the passage of the Privacy Act] intend to jeopardize the collection of intelligence information related to national defense or foreign policy, or open to inspection [classified information] to persons who do not have an appropriate security clearance or need to know.' (Senate Report 93-1183, p. 74)

The exemption provisions are permissive; that is, an agency is authorized, but not required, to exempt a system from all or any portion of selected provisions of the Privacy Act when an agency deems it to be in the best interest of the government and consistent with the act and the OMB Privacy Act Guidelines.[31]

Subsection (e)(6) of the Privacy Act requires that "prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to Subsection (b)(2) [the Freedom of Information Act (FOIA)] of this section, [the agency must] make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes."[32] While this requirement does not apply when information is being shared between Federal agencies, it is not a provision from which an agency can claim exemption. Consequently, an agency that has exempted records from Subsections (d) (access and amendment) and (e)(5) (accuracy, relevance, timeliness) of the act must nevertheless make reasonable efforts to ensure the accuracy, completeness, timeliness, and relevance of the records when it disseminates them outside the agency to authorized recipients, other than other Federal agencies and FOIA requesters.

An individual may bring a civil action against an agency under Subsection (g)(1)(C) of the Privacy Act if the agency "fails to maintain any record concerning [the] individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual."[33]

For guidance in interpreting and applying the Privacy Act's provisions, agencies should consult the Office of Management and Budget's (OMB) Privacy Act guidance and the case law interpreting the act.

In addition to review under the Privacy Act, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires all Federal agencies to inventory their holdings of personally identifiable information and to undertake the following data quality review:

---

[31] The OMB Privacy Act Guidelines, 40 *Federal Register* at 28,971, reflect the need for the exercise of agency discretion. In commenting on this provision, the House Committee noted:

> The Committee also wishes to stress that this section is not intended to require the CIA and criminal justice agencies to withhold all their personal records from the individuals to whom they pertain. We urge those agencies to keep open whatever files are presently open and to make available in the future whatever files can be made available without clearly infringing on the ability of the agencies to fulfill their missions. (House Report 93-1416, p. 19)

[32] 5 U.S.C. § 552a(e)(6).

[33] 5 U.S.C. § 552a(g)(1)(C).

> Review Current Holdings. Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.…
>
> Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agency's annual review and any consolidated publication of minor changes of Privacy Act systems of records notices.

The following is a list of authorities that may assist ISE participants in developing their data quality policies and procedures for PI in the ISE:

Statutes

Privacy Act of 1974, 5 U.S.C. § 552a. http://www.usdoj.gov/oip/privstat.htm

The Information Quality Act, 44 U.S.C. §§ 3504(d)(1) and 3516. (See OMB, *Information Quality: A Report to Congress*, April 30, 2004, detailing implementation of the IQA during Fiscal Year 2003. http://www.whitehouse.gov/omb/inforeg/fy03_info_quality_rpt.pdf (See also Congressional Research Service, *The Information Quality Act: OMB's Guidance and Initial Implementation*, September 17, 2004, CRS-2). http://www.it.ojp.gov/documents/CRS_IQ_Act_OMB_Guidance_and_Implementation.pdf.

Health Insurance Portability and Accountability Act of 1996 (HIPAA), August 21, 1996. http://aspe.hhs.gov/admnsimp/pl104191.htm

Gramm-Leach-Bliley Act (GLB),15 U.S.C. § 6801. http://www.ftc.gov/privacy/glbact/glbsub1.htm

Paperwork Reduction Act, Public Law 104-13, 44 U.S.C. § 3501 *et seq*. http://www.archives.gov/Federal-register/laws/paperwork-reduction/

National Archives and Records Administration, 44 U.S.C. § 2101 *et seq*. http://www.archives.gov/about/laws/nara.html#def (enabling legislation requiring NARA to determine data retention issues).

Regulations and Guidelines

Office of Management and Budget (OMB) *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies;*

Republication, 67 *Federal Register* No. 36, at 8452-60.
http://www.whitehouse.gov/omb/fedreg/reproducible2.pdf

28 CFR Part 23. http://www.it.ojp.gov/documents/28CFR_Part_23.PDF (requirements for Crime Control Act-funded criminal intelligence systems).

Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"), 45 CFR Parts 160 and 164. http://www.hhs.gov/ocr/combinedregtext.pdf

Gramm-Leach-Bliley Privacy Regulations, 16 CFR Part 313, 65 *Federal Register* 33646 (May 24, 2000). http://www.infolinkscreening.com/InfoLink/Resources/LegalIssues/PrivacyIssues.pdf

Policy Guidance and Standards

OMB *Privacy Act Implementation, Guidelines and Responsibilities*, 40 *Federal Register* 28948, 28965 (July 9, 1975). http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf

Implementation of the Privacy Act of 1974, Supplemental Guidance, 40 *Federal Register* 56741, (December 4, 1975). http://www.whitehouse.gov/omb/inforeg/implementation1974.pdf

Appendix I to OMB Circular No. A-130, *Federal Agency Responsibilities for Maintaining Records About Individuals*. http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.html

OMB *Privacy Act Guidance—Update* (May 24, 1985). http://www.whitehouse.gov/omb/inforeg/guidance1985.pdf

Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 *Federal Register* 25818 (June 16, 1989).
http://www.whitehouse.gov/omb/inforeg/final_guidance_pl100-503.pdf

OMB M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management* (June 13, 2005).
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-15.html

OMB M03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 26, 2003).
http://www.whitehouse.gov/omb/memoranda/m03-22.html

OMB M-01-05, *Guidance on Inter-Agency Sharing of Personal Data—Protecting Personal Privacy*, (December 20, 2000). http://www.whitehouse.gov/omb/memoranda/m01-05.html

OMB M-99-05, *Instructions on Complying With President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"* (January 7, 1999). http://www.whitehouse.gov/omb/memoranda/m99-05.html

OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*. http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.html

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf (requiring Federal agencies to review their data holdings and ensure data quality requirements are being met).

DOJ Overview of the Privacy Act of 1974. http://www.usdoj.gov/oip/04_7_1.html (links to discussion and citations to court decisions interpreting agency Privacy Act of 1974 data quality requirements).

DOJ's Global Justice Information Sharing Initiative, *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* (February 2008), at p. 20. http://www.it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf

DOJ's Global Justice Information Sharing Initiative, *Privacy Policy Development Guide and Implementation Templates*, at pp. 7–11, October 2006. http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

DOJ's Global Justice Information Sharing Initiative, Global Privacy and Information Quality Working Group, *Privacy and Information Quality Policy Development for the Justice Decision Maker* (September 2005). https://it.ojp.gov/documents/200411_global_privacy_document.pdf

DOJ's Global Justice Information Sharing Initiative, *Information Quality: The Foundation for Justice Decision Making* (February 2007). https://it.ojp.gov/documents/IQ_Fact_Sheet_Final.pdf

DOJ's Global Justice Information Sharing Initiative, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Illinois IJIS Privacy Policy Subcommittee report on *Privacy Issues Confronting the Sharing of Justice Information in an Integrated Justice Environment*, at p. 3 (October 2005). http://www.icjia.state.il.us/iijis/public/pdf/PRV/PRV_commiteeIssues_September2006.pdf

DOJ Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, at p. 24. http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf (discussing data quality issues at the Terrorist Screening Center).

U.S. Government Accountability Office (GAO), *Agency and Reseller Adherence to Key Privacy Principles* (April 2006). http://www.gao.gov/highlights/d06421high.pdf

GAO, *Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data* (June 2006). http://www.gao.gov/highlights/d06674high.pdf

GAO Highlights, *Agencies and Resellers Vary in Providing Privacy Protections* (April 2006). http://www.gao.gov/new.items/d06609t.pdf

Other GAO privacy-related testimony and reports can be found at: http://www.gao.gov/docsearch/app_processform.php?app_id=docdblite_topicsearch&submit=search&topic_search=Privacy

RESOURCES AND TOOLS

In crafting any needed ISE data quality policies and procedures for protected information (PI) in the ISE, agencies may wish to adopt some of the following suggested approaches and considerations:

1. Consider whether data quality reviews conducted pursuant to other requirements are current and appropriate in the ISE context, such as:
   a. Computer Matching Agreement
   b. Privacy Impact Assessment
   c. Memorandum of Understanding
   d. OMB Memorandum M-07-16 (May 22, 2007)

2. Articulate a process to identify priority areas for data quality review, such as:
   a. PI residing in systems of records subject to the data quality requirements of the Privacy Act (i.e., records that are not exempt from the Privacy Act's data quality requirements).
   b. PI residing in information systems subject to the data quality requirements contained in international agreements.
   c. Circumstances in which an erroneous record could result in an erroneous decision (versus circumstances permitting a range of accuracy).
   d. Circumstances in which subjective findings are critical and assessment of the author's expertise bears on a determination regarding data quality.

3. Articulate a process to evaluate PI in context with other existing records to detect inconsistencies or other concerns about accuracy.

4. Articulate a process for evaluating the integrity of data matching and merging activities vis-à-vis the identity of the record subject.

5. Articulate a process for correcting, supplementing, or annotating erroneous or deficient PI reported to the agency ISE Privacy Official (regardless of any exemption from data quality standards that may apply).

6. Articulate a process to prevent the use or dissemination of erroneous or deficient PI.

7. Articulate a process to notify a providing or receiving agency's ISE Privacy Official of errors, changes, clarifying or contrary information, or information alerting the recipient agency to possible limitations on the accuracy of the data, such as:

a. Including contrary or qualifying information in order to clarify the information in the record.
b. Clearly identifying opinions as such.
c. Identifying and advising recipients regarding records that are of questionable accuracy or have known limits on their accuracy[34] (see also Notice Mechanisms Guidance).
d. Including in the record a concise statement of any disagreement submitted by a record subject, when appropriate.[35]
e. Providing the last date on which the record was reviewed for accuracy.

8. Articulate a process to ensure timeliness of records maintained and shared, such as:
   a. Refraining from disseminating information known to be outdated.[36]
   b. Revisiting data retention schedules to determine whether shorter retention periods will reduce the number of outdated or irrelevant records.[37]
   c. Developing procedures for handling criminal history record information that has been sealed or expunged by court order.

9. Articulate a process to create an accounting of data quality reviews, identifying the reviewer and dates of correction/notice to providing or recipient agency ISE Privacy Officials.

[34] OMB Guidelines, *supra*, at 40 *Federal Register* 28965.

[35] *Id*. at 28959.

[36] Illinois IJIS Privacy Policy Subcommittee report on *Privacy Issues Confronting the Sharing of Justice Information in an Integrated Justice Environment*, at p. 3 (September 2006) (hereafter "Illinois IJIS Privacy Policy Subcommittee"). http://www.icjia.state.il.us/iijis/public/pdf/PRV/PRV_commiteeIssues_September2006.pdf

[37] Illinois IJIS Privacy Policy Subcommittee, *supra*, at p. 3.

DATA SECURITY

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 6, provide the following Data Security requirement:

> Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

To ensure the viability of the ISE and its use for the purposes intended, protected information[38] and associated information technology systems must be safeguarded from unauthorized access, disclosure, modification, use, or destruction.

The governing legal and regulatory security framework prescribes the process for determining the information security categories and associated information security controls applicable in specific operating environments. This legal and regulatory framework establishes the core elements for agency information assurance policies.

This guidance identifies the security standards that apply to Federal civilian, military, and intelligence information systems.

[38]Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

Core Elements

1. Non-National Security Systems
   a. Security categorization standards (low-, moderate-, high-impact)
      - *Standards for the Security Categorization of Federal Information and Information Systems* (NIST/FIPS 199)
   b. Minimum security requirements (keyed to system impact category)
      - *Minimum Security Requirements for Federal Information and Information Systems* (NIST/FIPS 200)
   c. Implementation of controls (keyed to minimum security requirements)
      - *Recommended Security Controls for Federal Information Systems* (NIST/SP 800-53)

2. National Security Systems
   a. Defense Information Assurance Certification/Accreditation Process (DIACAP)
   b. National Information Assurance Certification/Accreditation Process (NIACAP)
   c. Director of Central Intelligence Directive (CID) 6/3 (*Protecting Sensitive Compartmented Information Within Information Systems*)
   d. National Information Assurance Policy No. 11 (NSTISSP No. 11)

BACKGROUND AND COMMENTARY[39]

Introduction:

Section 6 of the ISE Privacy Guidelines provides the following Data Security requirement:

> Each agency shall use appropriate physical, technical, and administrative measures as required by law and policy to safeguard protected information in the ISE from unauthorized access, disclosure, modification, use, or destruction.

All Federal government systems involved in the ISE operate within environments that impose specific physical, technical, and administrative requirements that will be applicable to protected information (PI) shared in the ISE. Therefore, the purpose of this document is to identify the applicable computer-security requirements and suggest that participants in the ISE renew their focus and attention to this critical issue in order to safeguard PI in the ISE from unauthorized access, disclosure, modification, use, or destruction.

Federal Information and Information System Security Requirements

The Federal Information Security Management Act (FISMA) of 2002 (Title III of the E-Government Act of 2002) requires that all Federal agencies develop and implement agency-wide information security programs. Different types of systems, however, are governed by different security regimes. FISMA requires that all agencies protect Federal information and information systems in any format (electronic, paper, etc.) and follow the standards and guidelines[40] developed by the National Institute of Standards and Technology (NIST).[41] FISMA,

---

[39]The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. It is not a binding interpretation of law, regulation, or policy.

[40]Under certain circumstances, other Federal statutes may impose general security requirements on Federal agencies. These regulations and any new controls they create do not preclude agency responsibilities to implement FISMA. For example, the Privacy Act of 1974 requires that agencies that maintain information in a system of records must:

> Establish appropriate administrative, technical, and physical safeguards to insure [*sic*] the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. 5 U.S.C. § 552a(e)(10)

Additionally, there exist "sectoral" regulations that impose security requirements on entities that handle specific types of information; e.g., health, financial, and criminal intelligence. See *Health Insurance Reform: Security Standards; Final Rule* (a.k.a. the HIPAA Security Rule), 45 CFR Parts 160, 162, and 164 ("standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers"), at http://www.hipaadvisory.com/regs/finalsecurity/finalsecurity.txt; Gramm-Leach-Bliley *Standards for Safeguarding Customer Information; Final Rule*, 16 CFR Part 314 (establishing "standards relating to administrative, technical, and physical information safeguards for financial institutions subject to" Federal Trade Commission jurisdiction) at http://www.ftc.gov/os/2002/05/67fr36585.pdf; and Criminal Intelligence System Operating Policies, 28 CFR §23.20(g), which impose information security requirements on Crime Control Act-funded criminal intelligence systems. http://www.iir.com/28cfr/guideline.htm

[41] "NIST is a non-regulatory Federal agency in the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science,

however, exempts national security systems, as defined in 44 U.S.C. § 3542(b)(2), from NIST requirements. Per National Security Directive No. 42, national security systems are governed by security policies issued by the Committee on National Security Systems and the Director of the National Security Agency. Therefore, this paper will address applicable security requirements for (1) non-national security systems and (2) national security systems.

1. Non-National Security Systems

FISMA required NIST to develop Federal security categorization standards for Federal information and information systems according to impact levels. Therefore, in February of 2004, NIST issued Federal Information Processing Standards (FIPS) 199, *Standards for the Security Categorization of Federal Information and Information Systems*. FIPS 199 requires that agencies categorize their information systems as low-impact, moderate-impact, or high-impact as a starting point for ensuring the confidentiality, integrity, and availability of information in the system.

After agencies categorize their system security needs using FIPS 199, they are required to follow the mandatory security requirements contained in FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. FIPS 200 provides minimum security requirements for Federal information and information systems and establishes a risk-based process for determining the security controls necessary to ensure compliance with those requirements.

2. National Security Systems

As mentioned previously, FISMA specifically exempts national security systems from NIST requirements.[42] FISMA defines the term *national security system* at 44 U.S.C. § 3542(b)(2). NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System* (August 2003), assists agencies in identifying when they are operating a national security system.

---

standards, and technology in ways that enhance economic security and improve our quality of life." http://www.nist.gov/public_affairs/general2.htm

[42]"Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by Section 3542(b)(2) of Title 44, United States Code." *See* 44 U.S.C. § 3549(c)(1).

Agencies that deploy national security systems generally follow one of two different security methodologies: DoD Information Assurance Certification and Accreditation Process (DIACAP) or National Information Assurance Certification and Accreditation Process (NIACAP). With respect to certain types of intelligence information, agencies are also required to meet the security requirements contained in Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information Within Information Systems.*[43]

a. **DIACAP**

DIACAP[44] is the U.S. Department of Defense (DoD) information assurance (IA) certification and accreditation (C&A) process. DIACAP applies to both classified and unclassified[45] DoD information systems.[46] DIACAP is generally used only by defense agencies,[47] but civilian agencies sometimes apply DIACAP principles to their own C&A processes when not inconsistent with NIST guidance.

b. **NIACAP**

NIACAP is based on the National Security Telecommunications and Information System Security Instruction known as NSTISSI No. 1000.[48] NIACAP establishes the minimum national standards for certifying and accrediting certain national security systems. It is used in some form by the U.S. Department of State (http://www.state.gov/m/irm/rls/rm/21907.htm), the U.S. Department of the Treasury, the U.S. Department of Energy, the U.S. Department of Justice, and others as the methodology for protecting their national security systems. NIACAP is not used by DoD or members of the Intelligence Community who process Sensitive Compartmentalized Information (SCI).

[43]This document can be found at http://ftp.fas.org/irp/offdocs/DCID_6-3_20Manual.htm.

[44]DITSCAP was DIACAP's predecessor methodology. DIACAP superseded DITSCAP.

[45]FISMA specifically exempts DoD unclassified systems from the NIST guidance requirements that generally apply to unclassified systems. *See* 44 U.S.C. § 3543(c)(1).

[46]DoD Instruction Number 5200.40, at 2, § 2.3 ("Shall apply to the acquisition, operation and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information. It applies to any IT or information system life cycle, including the development of new IT systems, the incorporation of IT systems into an infrastructure, the incorporation of IT systems outside the infrastructure, the development of prototype IT systems, the reconfiguration or upgrade of existing systems, and legacy systems.")

[47]DITSCAP "[a]pplies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"), their contractors, and agents." DoD Instruction Number 5200.40, *Information Technology Security Certification and Accreditation Process (DITSCAP*), at 2, December 1997.

[48]This document can be found at http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf.

c. Central Intelligence Directive 6/3

The Director of Central Intelligence issued Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*[49] to establish uniform security guidance and requirements for ensuring adequate protection of Sensitive Compartmentalized Information (SCI) and information used in Special Access Programs (SAPs). SCI refers to a method by which certain types of classified information must be handled. It applies primarily to information regarding national security issues or programs that have not yet been publicly acknowledged. SAPs are programs that require extraordinary security requirements.[50]

[49]This document can be found at http://ftp.fas.org/irp/offdocs/DCID_6-3_20Manual.htm.

[50]Army Regulation 380–381, *Special Access Programs*, at http://www.fas.org/irp/doddir/army/ar380-381-old.pdf, provides the following examples of SAPs: (1) a specific technology with potential for weaponization that gives the United States a significant technical lead or tactical advantage over potential adversaries; (2) sensitive technology that is especially vulnerable to foreign intelligence exploitation without special protection; (3) an emerging technology, proposed operation, or intelligence activity risking the compromise of other SAPs; (4) exposure of sensitive activities that could jeopardize the lives of U.S. citizens; (5) a capability that is so unique or sensitive that it requires protection beyond normal procedures; (6) an extremely sensitive activity requiring special protection from disclosure to prevent significant damage to national security or the reputation or interests of the United States; (7) methods used to acquire foreign technology or equipment; and (8) sensitive support to DOD and non-DOD agencies.

The following is a list of authorities that may assist ISE participants in developing their data security policies and procedures for PI in the ISE:

Statutes

Privacy Act of 1974, 5 U.S.C. § 552a(e)(10) (requiring that system of records owners establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records).
http://www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552----000-.html

Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 *et seq.* (requiring civilian Federal information systems to follow computer security guidance issued by the National Institute of Standards and Technology [NIST]).
http://www4.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003541----000-.html

Clinger-Cohen Act of 1996, 40 U.S.C. § 1401 *et seq*., Public Law 104-106, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104 as amended by Public Law 104-208, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ208.104.pdf, which amended Public Law 104-106.

Regulations

Health Insurance Reform: Security Standards; Final Rule (a.k.a. the HIPAA Security Rule), 45 CFR Parts 160, 162, and 164 ("standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers"). http://www.hipaadvisory.com/regs/finalsecurity/finalsecurity.txt

Gramm-Leach Bliley *Standards for Safeguarding Customer Information; Final Rule*, 16 CFR Part 314, (establishing "standards relating to administrative, technical, and physical information safeguards for financial institutions subject to" Federal Trade Commission jurisdiction).
http://www.ftc.gov/os/2002/05/67fr36585.pdf

28 CFR § 23.20(g) (imposing security requirements on criminal intelligence systems).
http://www.it.ojp.gov/documents/28CFR_Part_23.PDF

Policy Guidance and Standards

NIST Publications.
http://www.nist.gov/public_affairs/pubs.htm

OMB Circular A-130 *Management of Federal Information Resources*, http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf, and OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf

DoD Instruction Number 5200.40.
http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/i520040p.pdf

National Information Assurance Certification and Accreditation Process (NIACAP).
http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf

Director of Central Intelligence Directive 6/3: *Protecting Sensitive Compartmented Information Within Information Systems*.
http://ftp.fas.org/irp/offdocs/DCID_6-3_20Manual.htm

National Information Assurance Acquisition Policy (NSTISSP No. 11).
http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf

National Security Directive No. 42.
http://www.cnss.gov/Assets/pdf/CNSSD-900.pdf

RESOURCES AND TOOLS

The following information may assist agencies in reviewing their policy issuances and compliance directives regarding the data security requirements appropriate to their operating environments:

Definition of National Security System (NSS):

1. Federal Information Security Management Act (FISMA) of 2002 (Title III of the E-Government Act of 2002), 44 U.S.C. § 3542(b)(2):
   a. Definition—In this subtitle, the term *national security system* means any telecommunications or information system operated by the United States government,
      (i) The function, operation, or use of which—
         (a) Involves intelligence activities;
         (b) Involves cryptologic activities related to national security;
         (c) Involves command and control of military forces;
         (d) Involves equipment that is an integral part of a weapon or weapons system; or
         (e) Subject to Subsection (b), is critical to the direct fulfillment of military or intelligence missions.
      (ii) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
   b. Limitation—Subsection (b)(2)(i)(e) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

2. DIACAP
   a. Applies to unclassified, as well as to classified DoD information systems.
   b. Civilian agencies often apply DIACAP principles to certification and accreditation processes when not inconsistent with NIST guidance.

3. NIACAP
   a. Agencies following NIACAP to certify and accredit NSSs include but are not limited to:
      i. U.S. Department of State (blended with NIST guidance)
      ii. U.S. Department of the Treasury
      iii. U.S. Department of Energy
      iv. U.S. Department of Justice

b. NIACAP is not appropriate for application to systems administering Sensitive Compartmentalized Information (SCI), such as those residing within DoD or at the various Intelligence Community agencies.

4. DCID 6/3
   - Applicable to information systems administering Sensitive Compartmentalized Information (SCI) and information used in Special Access Programs (SAPS).

5. NSTISSP-11
   - Applicable to the acquisition of information technology products for all systems entering, processing, storing, displaying, or transmitting national security information.

ACCOUNTABILITY, ENFORCEMENT, AND AUDIT

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 7, provide the following Accountability, Enforcement, and Audit requirements:

a. *Procedures.* Each agency shall modify existing policies and procedures or adopt new ones, as appropriate, requiring the agency to:

   (i) Have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;
   (ii) Provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information and, as appropriate, for reporting violations of agency privacy-protection policies;
   (iii) Cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and
   (iv) Designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

b. *Audit*. Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

The policies, procedures, and mechanisms governing the ISE are designed to protect the privacy and other legal rights of Americans and to ensure the timely availability and utility of protected information. To ensure these ends are achieved, agencies are encouraged to integrate enhanced accountability, enforcement, and audit policies and practices for protected information (PI)[51] in the ISE with existing agency compliance verification mechanisms. Where necessary, agencies should develop compliance verification mechanisms specific to their ISE activities. In either case, to ensure an adequate compliance policy/program, agencies should consider incorporating the following core elements:

Core Elements

1. Policy framework that addresses:
   a. Training of personnel authorized to handle PI in the ISE.
   b. Reporting of violations of agency privacy protection policies.
   c. Investigating identified/reported violations of agency privacy protection policies.
   d. Responding to identified/reported violations of agency privacy protection policies.
   e. Cooperating with audits and reviews by appropriate internal and external audit and oversight authorities.
   f. Measures ensuring that the agency ISE privacy official receives copies of all reports/notices regarding alleged errors in PI content that the agency has disseminated in the ISE.

2. Audit:
   Program review framework/inspection process for examining compliance with the ISE Privacy Guidelines in the following areas (ISE Privacy Guidelines section identified):
   a. Compliance with laws [Section 2]
      (Compliance with general and specific laws applicable to the agency)
   b. Purpose limitation (terrorism-related) [Section 3]
   c. Identification of PI [Section 4(a)]
   d. Notice mechanisms [Section 4(b)]
   e. Data quality [Section 5]
   f. Data security [Section 6]
   g. Accountability, enforcement, and audit [Section 7]

[51] Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

h.	Redress	[Section 8]
i.	Execution, training, and technology	[Section 9]
j.	Public awareness of agency policies and Procedures	[Section 10]

BACKGROUND AND COMMENTARY[52]

Purpose

The purpose of this document is to identify and discuss potential methods and tools that will enable agencies to comply with the accountability, enforcement, and audit requirements set forth in Section 7 of the ISE Privacy Guidelines. There are many existing Federal requirements and processes that agencies can use to conduct effective audit and oversight of compliance with the ISE Privacy Guidelines:

1. Identify the Persons Assigned to Privacy and Civil Liberties Roles:
   a. Section 12(a) of the ISE Privacy Guidelines requires that "[e]ach agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or Executive Order, or as otherwise identified in response to the Office of Management and Budget (OMB) Memorandum M-05-08[53] dated February 11, 2005), shall [unless another official is better situated to perform this role] directly oversee the agency's implementation of and compliance with these Guidelines (ISE Privacy Official)."[54]
   b. The ISE Privacy Guidelines further state that the ISE Privacy Official shall be responsible for ensuring that "(i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these guidelines, and (ii) changes are made as necessary."[55]
   c. In most instances, the ISE Privacy Official's duties will be handled by each agency's statutory privacy officer or the person appointed as the Senior Agency Official for Privacy (SAOP) under OMB M-05-08. Some agencies, however, also

[52] The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. It is not a binding interpretation of law, regulation, or policy.

[53] OMB Memorandum 05-08 (M-05-08), *Designation of Senior Agency Official for Privacy*, requires that each executive department and agency appoint a Senior Agency Official for Privacy to oversee privacy development and implementation. OMB guidance specifically requires that the Official's role "include reviewing the agency's information privacy procedures to ensure that they are comprehensive and up-to-date, and where additional or revised procedures may be called for, working with the relevant agency offices in the consideration, adoption, and implementation of such procedures." OMB M-05-08 also requires that this official review existing departmental and component-level privacy policies and procedures to: "ensure the agency's full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act."

[54] ISE Privacy Guidelines, Section 12(a).

[55] "The ISE Privacy Official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's [senior ISE official]." ISE Privacy Guidelines, Section 12(a).

have separate components (e.g., the U.S. Department of Homeland Security [DHS] Office for Civil Rights and Civil Liberties) that handle civil rights and civil liberties issues (e.g., racial profiling) that are beyond the scope of the duties of statutory and OMB-required privacy officials. In addition to appointing an ISE Privacy Official, these agencies may want to consider appointing an ISE point person from civil rights and civil liberties offices where those functions are separate from the SAOP or the statutory privacy officer duties.

2. Leverage Existing Agency Training Programs:
   a. OMB M-05-08 privacy officials (who have assumed the role of ISE Privacy Official in most agencies) are also required to "ensure the agency's employees and contractors receive appropriate training and education regarding the information privacy laws, regulations, policies, and procedures governing the agency's handling of personal information."
   b. Agencies generally provide specialized training with respect to one or more of the following: Privacy Act, Freedom of Information Act, E-Government Act, the handling of Sensitive but Unclassified (proposed as Controlled Unclassified Information [CUI]) and classified information, and/or computer security requirements.
   c. These existing training procedures could be enhanced, where necessary, to do the following:
      i. Ensure employee awareness of proper access, use, and disclosure of PI in the ISE.
      ii. Provide training for personnel in agency policies for reporting noncompliance with agency-developed ISE policies and procedures.
      iii. Ensure that employees are aware of penalties for misuse of information in the ISE.
      iv. Use existing or develop modified agency policies for reporting violations of agency ISE privacy and other civil liberties protection policies to designated authorities within the agency.

3. Leverage Existing Internal Agency Processes, Policies and Procedures, and Oversight Resources:
   a. Processes. Existing privacy and other review processes and resources could be leveraged as part of ISE oversight, such as:
      i. Information sharing review boards or councils.
      ii. Privacy Impact Assessment processes.
      iii. Civil rights and civil liberties office review (where separate from the M-05-08 or Privacy Officer functions).

iv. Data integrity boards.
v. National Security Systems participating in the ISE can leverage the security controls, safeguards, standards, and countermeasures being defined by both the Committee on National Security Systems (CNSS) and the Director of National Intelligence (DNI) Certification and Accreditation (C&A) Transformation initiatives. These initiatives embrace the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) as outlined in Special Publication 800.53.

b. Policies and Procedures. Existing policies and procedures regarding the handling, sharing, and use of sensitive information may provide for oversight, audit, and accountability for PI, but if they do not, they should be amended to provide needed policies and procedures. Where necessary and as appropriate, these amendments could provide for the following with respect to information used and shared in the ISE:
   i. Maintenance of records that are available for reasonable audit and inspection by appropriate officials or entities.[56]
   ii. "[I]nspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency criminal intelligence information."[57]
   iii. Encouragement of active agency employee participation in oversight, enforcement, auditing, and compliance.
   iv. Periodic reviews of the content of PI disseminated and received in the ISE in order to ensure compliance with the ISE Privacy Guidelines.
   v. Random auditing of audit trails and other information maintained regarding the agency's use and dissemination of PI in the ISE.[58]

c. Oversight Resources. Agency Inspectors General—In addition to ISE privacy officials (who will generally have oversight but not auditing functions), most of

[56] Agency-specific authorities and mission may determine the information to be captured in transaction logs; i.e., the operations, recipients, or communications about which the agency will maintain auditable records. For example, U.S. Department of Justice-funded systems maintaining "criminal intelligence information" must maintain records indicating "who has been given information, the reason for release of the information, and the date of each dissemination." See 28 CFR § 23.20(g).

[57] See U.S Department of Justice, 28 CFR § 23.20(n), which states that:

> A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

[58] Institute for Intergovernmental Research, *28 CFR Part 23 Sample Operating Policies and Procedures,* http://www.iir.com/28cfr/SampleOperatingPolicies.pdf.

the Federal participants in the ISE have their own Inspector General's Office. The Inspectors General conduct and supervise audits and investigations relating to the programs and operations of the organizations for which they are responsible. They also recommend policies for activities designed to promote economy, efficiency, and effectiveness in the administration of the programs they oversee.[59]

i. Inspectors General can help to ensure that their agencies comply with the ISE Privacy Guidelines.

ii. Investigations of suspected violations should "focus principally on systemic measures to avoid future violations."[60]

4. Use Existing Tools Available for Implementing Audit and Review Mechanisms to Ensure Accountability, Enforcement, and Audit, such as strong audit trails.[61] As emphasized in the Markle Foundation report, strong audit trails (or logs) are needed to ensure protection of privacy and civil liberties in the ISE.[62] An audit trail is "a record showing who has accessed an IT system and what operations the user has performed during a given period."[63] The audit trail, primarily established for security purposes, allows the project [agency] to track the file, maintain compliance, and notify a recipient if it turns out there is invalid information in a file."[64]

[59] 5 U.S.C. § 1 *et seq*. http://www4.law.cornell.edu/uscode/html/uscode05a/usc_sup_05_5_10_sq2.html

[60] *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*, at p. 33. http://www.markle.org/downloadable_assets/nstf_part_1.pdf

[61] OMB M-07-16, May 22, 2007, Attachment 1 C, provides the following "Log and Verify" security requirement to prevent and identify breaches of sensitive Federal information: "Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required."

[62] "Consistent with a vigorous defense against terrorism, these guidelines envision tools that create audit trails of parties who carry out searches, that anonymize and minimize information to the greatest extent possible, and that prevent both the intentional and unintentional dissemination of irrelevant information to unauthorized persons or entities." *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*, at p. 33. http://www.markle.org/downloadable_assets/nstf_part_1.pdf

[63] NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems,* August 2002, at D-1. http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

[64] Institute for Intergovernmental Research, *Frequently Asked Questions Regarding 28 CFR Part 23*, FAQ Number 20. http://www.iir.com/28cfr/FAQ.htm#q20

5. Consider Using Emerging Tools and Technologies:
   There are many emerging technologies to assist agencies in tracking the ISE in order to ensure accountability, provide enforcement, and enhance auditing capabilities. Technologies that ISE participants may consider include, but are not limited to:
   a. Permissioning systems
   b. Hashing
   c. Data anonymization
   d. Immutable Audit logs[65]
   e. Authentication[66]

   These tools and technologies may be considered when conducting system development and in the development or modification of agency policies designed to ensure compliance with the ISE Privacy Guidelines.

The following is a list of authorities that may assist ISE participants in developing their accountability, enforcement, and audit policies and procedures for PI in the ISE:

Statutes

Inspector General Act of 1978, 5 U.S.C. § 1 *et seq*.
http://www4.law.cornell.edu/uscode/html/uscode05a/usc_sup_05_5_10_sq2.html

Regulations

28 CFR § 23.20 (requiring that projects maintaining criminal intelligence information ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to ensure against unauthorized access and against intentional or unintentional damage).
http://www.it.ojp.gov/documents/28CFR_Part_23.PDF

Policy Guidance and Standards

OMB Memorandum M-05-08 (February 11, 2005), *Designation of Senior Agency Officials for Privacy*, http://whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf (requiring that every Federal agency appoint a Senior Agency Official for Privacy to oversee privacy development, implementation, and oversight).

OMB Memorandum M-07-16 (May 22, 2007), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
28 CFR Part 23, Sample Operating Policies and Procedures.
http://www.iir.com/28cfr/SampleOperatingPolicies.pdf

---

[65]Markle Foundation, *Implementing a Trusted Information Sharing Environment, Using Immutable Logs to Increase Security, Trust, and Accountability* (2006). "Immutable logs are tamper resistant logs of user activity in the information sharing environment. Audit of immutable logs would allow authorized officials to trace the origin of a piece of information, who has accessed it, under what circumstances, pursuant to what authority, and how it actually has been used, thus providing a mechanism to oversee or measure compliance with privacy and security rules. As a mechanism for oversight and review of system usage, immutable logs are a key component of accountability." *Id.* at p, 70.
http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf

[66] ISE Privacy Guidelines, Section 9(c), Technology.

Commentators

Markle Foundation, *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*, at p. 33. http://www.markle.org/downloadable_assets/nstf_part_1.pdf (discussing accountability in the Information Sharing Environment).

Markle Foundation, *Implementing a Trusted Information Sharing Environment, Using Immutable Logs to Increase Security, Trust and Accountability* (2006) (discussing use of immutable audit logs to ensure accountability). http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf

J. Dempsey and P. Rosenzweig, *Technologies That Can Protect Privacy as Information Is Shared to Combat Terrorism* (May 26, 2004).
http://www.heritage.org/research/homelandsecurity/upload/63976_1.pdf

American Statistical Association, *Frequently Asked Questions Regarding the Privacy Implications of Data Mining* (includes discussion of permissioning systems).
http://www.amstat.org/profession/index.cfm?fuseaction=dataminingfaq#4

RESOURCES AND TOOLS

In developing a program review framework, agencies may find it expedient to add oversight of ISE-specific processes involving protected information (PI) in the ISE to the portfolios of agency offices/officials already responsible for maintaining and handling personally identifiable information (PII). ISE-specific processes that may be merged into existing PII handling functions include:

1. Access, use, and disclosure of PI.
2. Training regarding the access, use, and disclosure of PI.
3. Maintenance of records/logs regarding access to/disclosure of/receipt of PI.
4. Review of compliance with PI handling policies and practices.
5. Investigation of reported/identified violations of PI handling practices.
6. Procurement/development of information technology for administering PI.
7. Audit, inspection, and investigation of agency programs.

The Office of the Director of National Intelligence has undertaken studies of existing and emerging privacy-enhancing technologies and will make the results available to agencies when completed.

Page intentionally left blank.

Appendix E
ISE Privacy Policy Outline

Page Intentionally Left Blank.

Information Sharing Environment (ISE) Privacy Policy Outline

I. Background and Applicability

In this section, agencies may describe or reference introductory information about their mission, relationship to the ISE, and purpose for establishing this policy. Agencies may also articulate the anticipated benefits of successfully having implemented this policy.

II. Compliance With Laws

In this section, agencies may consider including a statement regarding compliance with the Constitution and all applicable laws and Executive Orders relating to protected information.

In addition, agencies may describe their rules assessment process, including any legal restrictions applicable to protected information. Agencies subject to constraints on seeking and obtaining certain kinds of information may wish to represent that protected information has been lawfully obtained and shared.

III. Purpose Specification

In this section, agencies may consider including a description of internal policies and procedures that ensure that the agency's access to and use of protected information available through the ISE is consistent with the authorized purpose of the ISE.

IV. Identification of Protected Information to Be Shared Through the ISE

In this section, agencies may consider identifying data holdings that contain protected information to be shared in the ISE and describing the mechanisms, as feasible, to ensure protected information has been reviewed to meet the ISE Privacy Guidelines requirements.

In addition, agencies may consider including their notice mechanisms for enabling ISE participants to determine the nature of the information so the information can be handled appropriately.

- Agencies should reference the Appendix D—Key Issues Guidance on Notice Mechanisms to ensure the core elements are included in this section.

V. Data Quality

In this section, agencies may consider referencing or reproducing their policies and procedures to facilitate the prevention, identification, and correction of any errors in protected information so that information shared in the ISE is accurate and has not erroneously been shared through the ISE.

In addition, agencies may consider including the procedure for reporting errors when it is determined that information shared in the ISE originating from another agency contains erroneous information, including information incorrectly merged and information that lacks adequate context such that the rights of individual may be affected.

Also, agencies may consider referencing or reproducing policies and procedures that address:

- *Criteria for merging protected information about an individual from two or more sources;*

- *How alleged errors and deficiencies of protected information will be timely investigated and corrected, deleted, or "quarantined" from use; and*
- *How information will be retained only so long as it is relevant and timely for appropriate use by the agency, including procedures to update, delete, or "quarantine" protected information that is outdated or irrelevant.*

  - Agencies should reference Appendix D—Key Issues Guidance on Data Quality to ensure the core elements are included in this section.

VI. Data Security

In this section, agencies may consider reproducing or describing the physical, technical, and administrative measures they will use to safeguard protected information shared through the ISE.

  - Agencies should reference Appendix D—Key Issues Guidance on Data Security to ensure the core elements are included in this section.

VII. Accountability, Enforcement, and Audit

In this section, agencies may reference or describe internal policies and procedures that discuss:
- *Reporting, investigating, and responding to violations of agency policy;*
- *The training of personnel authorized to share protected information through the ISE; and*
- *Plans for audits and reviews with respect to the ISE.*

  - Agencies should reference Appendix D—Key Issues Guidance on Accountability, Enforcement, and Audit to ensure the core elements are included in this section.

VIII. Redress

In this section, agencies may reference or describe internal policies and procedures to address complaints from persons regarding protected information about them that is under agency control.

  - Agencies should reference Appendix D—Key Issues Guidance on Redress to ensure the core elements are included in this section.

IX. Execution, Training, and Technology

In this section, agencies may reference or describe internal policies and procedures for training, business process changes, and system designs intended to ensure that ISE privacy protections are implemented appropriately.

X. Awareness

In this section, agencies may reference or describe internal policies and procedures regarding anticipated steps for facilitating public awareness of activities to implement the ISE Privacy Guidelines.

XI. Non-Federal Entities

In this section, agencies may reference or describe policies and procedures for determining whether non-federal recipients of protected information have privacy protections "at least as comprehensive" as those specified in the ISE Privacy Guidelines. Agencies should focus on non-federal entities with which they have sharing arrangements, other than the fusion centers, because there is a mechanism in place to make that determination.

XII. Governance

In this section, an agency may identify the designated ISE Privacy Official responsible for ensuring the agency's compliance with the ISE Privacy Guidelines. In addition, an agency may consider including a description of any governance structure that is in place to handle ISE-related issues.

XIII. General Provisions

In this section, agencies may consider referencing or including any general provisions necessary for the successful implementation of the ISE Privacy Guidelines as well as definitions related to the ISE.

Page intentionally left blank.

Appendix F
Steps for Assessing Federal Agency Systems of Records

Page is intentionally left blank.

Steps for Assessing Federal Agency Systems of Records—Definitional Scope of the ISE Privacy Guidelines

This paper is designed to guide agencies through the process of applying the Information Sharing Environment (ISE) Privacy Guidelines to agency systems ("systems" is used herein to refer to information systems, databases, and data sets, as appropriate) containing protected information within the scope of the ISE, i.e., terrorism-related information.

Background

The suggested approach relies on the definitions of "terrorism information, including weapons of mass destruction (TI)," "homeland security (HS) information," and "law enforcement information related to terrorism (LE/T)"[67] (hereafter collectively referred to as terrorism-related information or TRI). Additionally, it recognizes the purpose and focus of the ISE Privacy Guidelines and their specific process requirements. The approach, described below, also acknowledges the ISE goal of facilitating, coordinating, and expediting access to protected information.

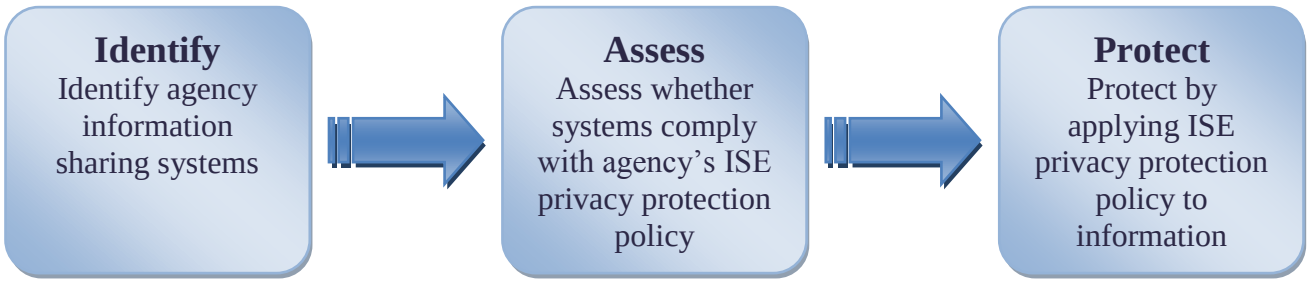
While the definitions in Guideline 2, Guideline 5, and the 9/11 Commission Act of 2007 clearly delineate the types of information covered both within the ISE and subject to the ISE Privacy Guidelines, additional guidance has been developed on how ISE Privacy Officials can apply these definitions to their agency's systems and sharing arrangements.

Agencies should understand that the ISE Privacy Guidelines apply to existing information sharing arrangements and systems as well as new information sharing arrangements and systems.

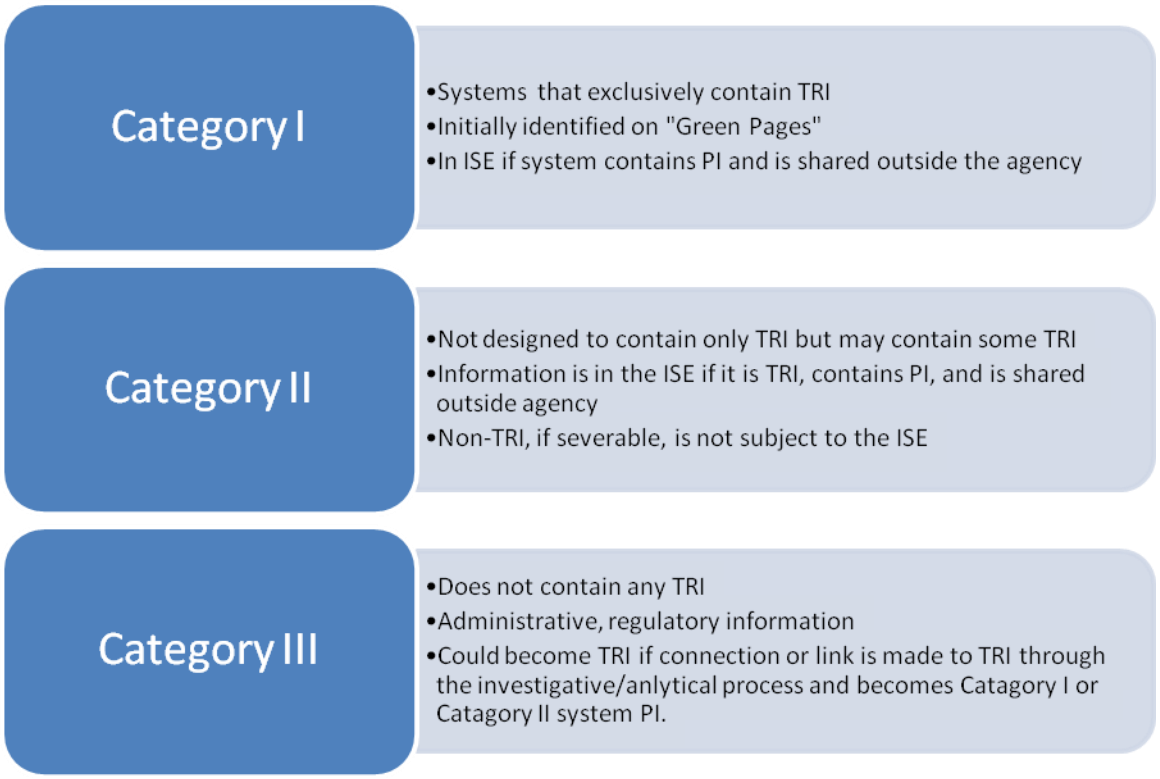
[67] As contained in Guideline 2—Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector (attached for reference), Guideline 5—Guidelines to Implement Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment (ISE Privacy Guidelines), and "Implementing Recommendations of the 9/11 Commission Act of 2007."

Approach

The *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment* (Implementation Guide) provides a recommended process when applying the ISE Privacy Guidelines to agency ISE privacy protection policies and information sharing arrangements and systems. However, prior to implementing the ISE Privacy Guidelines, privacy officials should identify their agency's information arrangements and systems and then assess the applicability of the systems under the ISE Privacy Guidelines (i.e., identify the type of information collected, stored, and shared within these systems). This initial step will assist agencies in effectively and efficiently applying the ISE Privacy Guidelines to covered information sharing arrangements and systems.



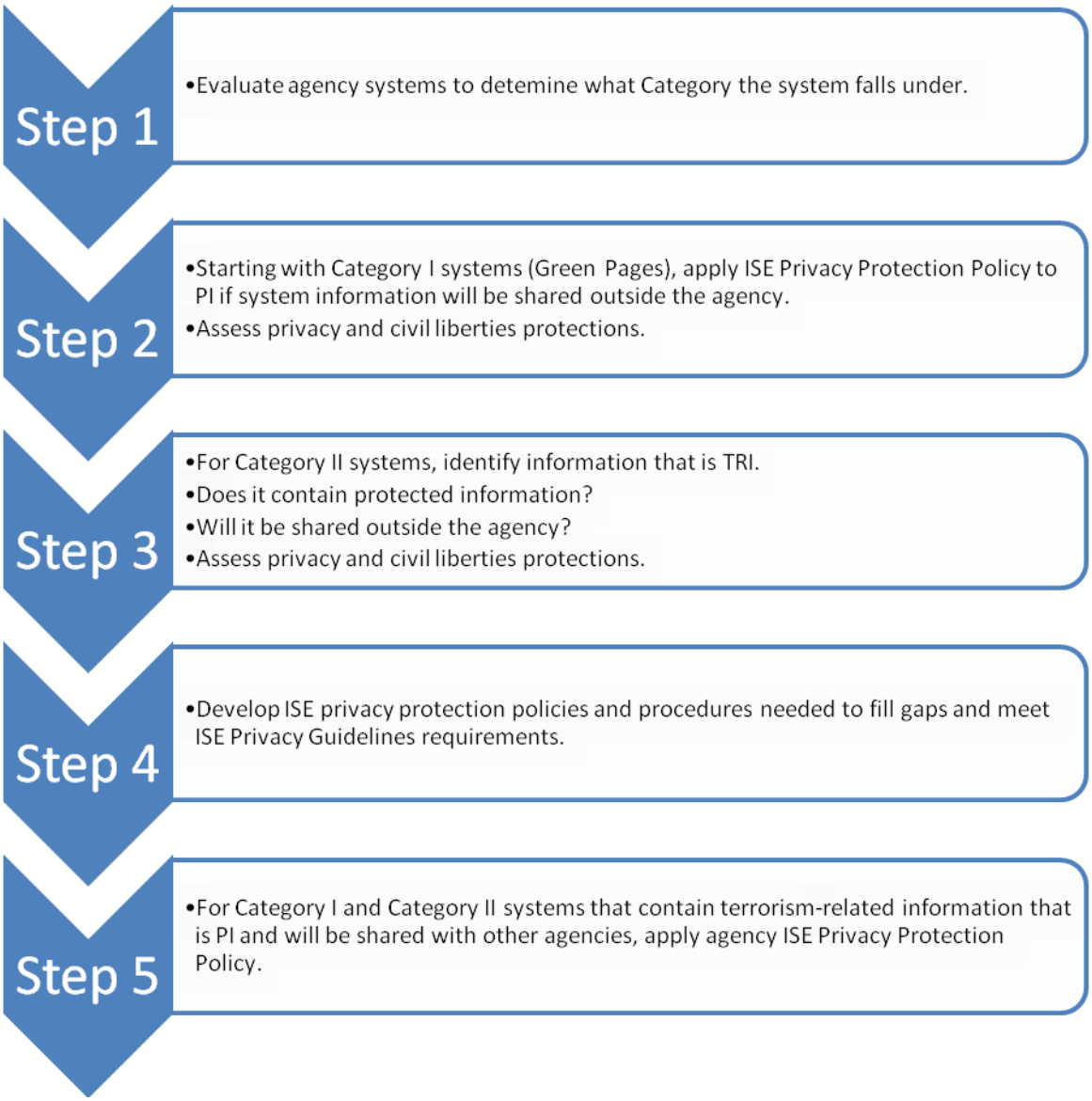
To assist in identifying systems that are subject to the ISE, three overarching system categories have been identified for agencies to utilize when initially assessing their systems. TRI is terrorism-related information as defined by the ISE Privacy Guidelines.



The first and third categories are relatively clear, and initial ISE Privacy Guidelines implementation should proceed on the basis that Category I systems are subject to the ISE Privacy Guidelines and that Category III systems are not covered by the ISE Privacy Guidelines. Requests for information from a Category III system should be handled on a case-by-case basis.

For purposes of applying the ISE Privacy Guidelines to Category II systems, a decision must first be made as to whether or not data meets the ISE parameters. The ISE Privacy Guidelines require that each agency identify its data holdings that contain protected information to be shared. In making determinations about Category II systems, privacy officials should address what, if any, system information is TRI, contains protected information (PI) that will be shared and, if shared, with whom it will be shared.

Follow these steps:



Page intentionally left blank.

Appendix G
Chart of Publicly Available Federal Privacy Policies

Page is intentionally left blank.

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of Housing and Urban Development (HUD)	**Privacy Act Handbook** http://www.hud.gov/offices/adm/hudclips/handbooks/admh/1325.1/index.cfm **Privacy Act Statement** http://www.hafresno.org/files/Federal_Privcy_Act_Statement_2004512-112747_.pdf **Privacy Act Regulations** http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=0edcc1de392289eff20df98b121d2825&tpl=/ecfrbrowse/Title24/24cfr16_main_02.tpl	**HUD Privacy Policy and Security Statement** http://www.hud.gov/assist/privacy.cfm **HUD PIA Guidance** http://www.hud.gov/offices/cio/privacy/pia/piaquestionnaire.doc		**HUD Privacy Principles** http://www.hud.gov/offices/cio/privacy/documents/privprin.pdf **Information Collection Reviews** http://www.hud.gov/offices/cio/rpm.cfm
U.S. Department of Education (ED)	**Privacy Act Issuances** http://www.ed.gov/policy/gen/leg/issuances.doc **Privacy Act Regulations** http://www.ed.gov/legislation/FedRegister/finrule/1999-2/060999a.html	**Web Site Privacy Policy** http://www.ed.gov/notices/privacy/index.html **Privacy Impact Assessments (PIA)** http://www.ed.gov/notices/pia/index.html		**Civil Liberties Guidance** http://www.ed.gov/about/offices/list/ocr/publications.html **Handbook for Protection of Sensitive But Unclassified Information** http://www.ed.gov/fund/contract/about/acs/acshbocio15.doc **Balancing Student Privacy and School Safety: A Guide to the** Family Educational Rights and Privacy Act **for Elementary and Secondary Schools** http://www.ed.gov/policy/gen/guid/fpco/brochures/elsec.html

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of Agriculture (USDA)	**Safeguarding Privacy Information**	**USDA Web Site Privacy Policy**		**Civil Liberties Redress**
	http://www.usda.gov/da/pdsd/Security%20Guide/S2unclas/Privacy.htm	http://www.usda.gov/news/privacy.htm		http://www.ascr.usda.gov/complaint_filing.html
	Collection of Information and Data (Privacy Act)	**Sample USDA Component Web Privacy Policies**		**Departmental Privacy Policy Brochure**
	http://www.rma.usda.gov/regs/collection.html	http://www.ers.usda.gov/AboutERS/Privacy.htm		http://www.usda.gov/documents/Looking_Privacy_Leaders_at_FSA.doc
	Where and How to Submit a Privacy Act Request	http://www.fsis.usda.gov/Privacy_Policy/index.asp		
	http://www.ascr.usda.gov/privacy_cr_submit.html	http://www.fns.usda.gov/fns/privacy.htm		
		http://www.csrees.usda.gov/about/privacy.html		
	Privacy Act FAQ	http://www.rma.usda.gov/web/privacy.html		
	http://www.ascr.usda.gov/faq/faq_privacy_cr.html	http://www.gipsa.usda.gov/GIPSA/webapp?area=home&subject=pp&topic=landing		
		http://www.fas.usda.gov/privacy.asp		
		http://www.rurdev.usda.gov/system.htm		
		http://www.ars-grin.gov/mia/Pages/Home/privacy.htm		
		http://www.aphis.usda.gov/privacy.html		
U.S. Department of Labor (DOL)	**Privacy Act Systems**	**DOL Privacy and Security Statement**		
	http://www.dol.gov/sol/privacy/main.htm	http://www.dol.gov/dol/privacynotice.htm		
	Privacy Act Systems—Universal Routine Uses of the Records	**Sample DOL Component Web Privacy Policies**		
	http://www.dol.gov/sol/privacy/intro.htm	http://www.doleta.gov/privacy.cfm		
		http://www.msha.gov/privacy.htm		
	Privacy Act Systems—Government-Wide Systems Controlled by DOL—Assertion of Authority			
	http://www.dol.gov/sol/privacy/gov-wide.htm			

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of Justice (DOJ)	**Overview of the Privacy Act of 1974**	**Web Site Privacy Policy Notice**		**Civil Liberties Redress**
	http://www.usdoj.gov/oip/04_7_1.html	http://www.usdoj.gov/privacy-file.htm		http://www.usdoj.gov/oig/FOIA/hotline2.htm
	FBI Privacy Act Request Instructions	**Sample DOJ Component Web Privacy Policies**		**Links to Federal Privacy Laws**
	http://foia.fbi.gov/privacy_instruc.htm			http://www.usdoj.gov/pclo/prr.htm
		http://www.fbi.gov/privacy.htm		
		http://www.usdoj.gov/atr/privacy.htm http://www.bop.gov/policy/privacypolicy.jsp		**Privacy Certificate and Confidentiality Requirements of National Institute of Justice (NIJ) Funding**
		http://www.ojp.gov/nij/funding/humansubjects/protection-privacy.htm		http://www.ojp.gov/nij/funding/humansubjects/privacy-certificate-instructions.htm
		Privacy Impact Assessment Guidance		**Privacy Certificate Guidance**
		http://www.usdoj.gov/pclo/pia.htm		http://www.ojp.gov/nij/funding/humansubjects/privacy-certificate-guidance.htm
				Model Privacy Certificate
				http://www.ojp.gov/bjs/pub/pdf/bjsmpc.pdf
				National Crime Prevention and Privacy Compact and Council Handbook
				http://www.fbi.gov/hq/cjisd/web%20page/pdf/cchandbook.pdf

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of State (State)		**Web Site Privacy Policy Notice**		**On-the-Record Briefing on Unauthorized Accessed Passport Records**
		http://www.state.gov/misc/87529.htm#privacy		http://www.state.gov/m/rls/102460.htm
		Privacy Impact Assessments and SORNs		**Safety and Security of U.S. Borders/Biometrics**
		http://www.state.gov/m/a/ips/c24170.htm		http://travel.state.gov/visa/immigrants/info/info_1336.html
				Office of Civil Rights
				http://www.state.gov/s/ocr/
U.S. Department of Health and Human Services (HHS)		**Web Site Privacy Policy Notice**		**HIPAA Privacy Rule**
		http://www.hhs.gov/Privacy.html		http://www.hhs.gov/ocr/hipaa/finalreg.html
				Privacy and Your Health Information
				http://www.hhs.gov/ocr/hipaa/consumer_summary.pdf
				Your Health Information Privacy Rights
				http://www.hhs.gov/ocr/hipaa/consumer_rights.pdf
				Protecting the Privacy of Patients' Health Information
				http://www.hhs.gov/news/facts/privacy2007.html
				How to File a Health Information Privacy Complaint
				With the Office For Civil Rights http://www.hhs.gov/ocr/privacyhowtofile.Htm

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of Transportation (DOT)	**Guide for Making Privacy Act Requests**	**Web Site Policy**	**DOT Cookie Use Checklist**	**Privacy Protection Manual**
	http://www.dot.gov/foia/index.html	http://www.dot.gov/privacy.html	http://cio.ost.dot.gov/staticfiles/DOT/OST/Documents/files/CookiesChecklistJan1.doc	http://cio.ost.dot.gov/DOT/OST/Documents/files/chapter8.doc
	Information Collection Clearance			
	http://cio.ost.dot.gov/portal/site/cio/informationcollection/index.html			
U.S. Department of Veterans Affairs (VA)	**Notice of Privacy Practices**	**Web Site Policy**	Eliminating the Unnecessary Collection and Use of Social Security Numbers at the Department of Veterans Affairs http://www.privacy.va.gov/docs/SSNPlanFinal9-17-07.pdf	**Privacy Service Fact Sheet**
	http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089	http://www.va.gov/Privacy/		http://www.privacy.va.gov/docs/Privacy_Service_Fact_Sheet.pdf
			Evaluating Holdings of Personally Identifiable Information (PII) and Eliminating Unnecessary Collections at the Department of Veterans Affairs	
	VA Code of Fair Information Practices	**Privacy Impact Assessment Guidance**	http://www.va.gov/oit/egov/rms/Files/PIIPlan07Section508.pdf	**VA Privacy Program**
	http://www.privacy.va.gov/docs/VA_Code_Of_Privacy_Principles.pdf	http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=53&FType=2		http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=51&FType=2
			Duties of VA Privacy Officers	
	Procedures for Processing Requests for Records Subject to the Privacy Act	**Privacy Impact Assessments**	http://www.privacy.va.gov/Privacy_Officers.asp	**Information Security Program**
	http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=23&FType=2f	http://www.privacy.va.gov/Privacy_Impact_Assessment.asp		http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=56&FType=2
			Privacy Violation Tracking System (PVTS) http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=52&FType=2	
	Procedures for Establishing and Managing Privacy Act Systems of Records http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=24&FType=2f			**Minimum Necessary Standard For Protected Health Information** http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=412
	Privacy and Release of Information			
	http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1423			

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of Defense (DoD)	**DoD Privacy Act Procedural Rules**	**DoD Privacy Impact Assessment (PIA) Guidance**	Safeguarding Against and Responding to the Breach of PII, http://www.defenselink.mil/privacy/pdfdocs/Safeguarding%20Against%20and%20Responding%20to%20the%20Breach%20of%20PII%20%20-%20OSD%2015041-07.pdf	DoD Privacy Program http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf
	http://www.defenselink.mil/privacy/cfr-rules.html	http://www.defenselink.mil/privacy/DoD_PIA_Guidance_Oct_28_2005.pdf		
			U.S. Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)	http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf
	Guidelines for Writing a New Privacy Act Statement or Notice	**Web Site Policy**	http://www.defenselink.mil/privacy/DoD_Guidance_on_%20Protecting_Personally_Identifiable_Information_Aug_26_2006.pdf	
	http://www.dod.mil/pubs/foi/privacy/newPAS.html	http://www.defenselink.mil/warning/warn-dl.html		**PRIVACY: Basic Principles**
				http://www.dod.mil/pubs/foi/privacy/basicprinciples.html
	System of Records Notice Review Template	**U.S. Marine Corps (USMC) Privacy Statement**		
	http://www.dod.mil/pubs/foi/privacy/System_Notice_Certification.xls	https://navalforms.daps.dla.mil/formsDir/NAVMC%2011000.PDF		**U.S. Department of the Navy Privacy Program**
				http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5211.5E.pdf
	U.S. Department of the Navy Privacy Training			
	http://privacy.navy.mil/training/			**Review of Safeguarding Policies and Procedures for Personnel-Related Data**
				http://www.dod.mil/pubs/foi/privacy/privacy_PIIPrimaryActionMemo_20070615.pdf

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of Homeland Security (DHS)		DHS Web Site Privacy Policy	Use of Social Security Numbers at the Department of Homeland Security http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-2.pdf	Privacy Technology Implementation Guide
		http://www.dhs.gov/xutil/gc_1157139158971.shtm		http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_ptig.pdf
		Transportation Security Administration (TSA) Web Site Privacy Policy	Privacy Incident Handling Guidance	DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons
		http://www.tsa.gov/research/reading/regs/editorial_1773.shtm	http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf	http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf
		Privacy Impact Assessment Official Guidance		
		http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf		DHS Traveler Redress Inquiry Program (DHS TRIP). http://www.tsa.gov/travelers/customer/redress/index.shtm
U.S. Department of Commerce (DOC)	IT Privacy Awareness Training http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/PROD01_002418	Sample Component Web Site Policies	Deputy Secretary's Memo on Safeguarding PII	
		http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/dev01_003747	http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/prod01_002739.pdf	
			Chief Information Officer's (CIO) Memo on Safeguarding PII	
			http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/prod01_002739.pdf	
			U.S. Department of Commerce Breach Notification Response Plan	
			http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/prod01_004786.pdf	
		Web Site Policy	Data Extract Log and Verify Requirement	Information Technology Privacy Policy
		http://www.commerce.gov/Privacy/index.htm	http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/prod01_005323.pdf	http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/DEV01_002682

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of Energy (DOE)	**Privacy Act Systems of Records**	**Web Site Policy**	**Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information**	**Information Collection Management Program**
	hhttp://www.management.energy.gov/Privacy Act_1974.pdf	http://www.energy.gov/privacy.htm	http://www.directives.doe.gov/cgi-bin/explhcgi?qry1059194691;doe-58	http://www.directives.doe.gov/cgi-bin/explhcgi?qry1349548267;doe-47
				http://www.directives.doe.gov/pdfs/doe/doetext/neword/200/o2002.pdf
		Department of Energy Procedures For Conducting Privacy Impact Assessments http://www.management.energy.gov/documents/PIAGuidance07-10-08.pdf	http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/n2065.html	
		Privacy Impact Assessment (PIA) Template		
		http://www.management.energy.gov/documents/PIATemplateRev7-21-08.pdf		
		Completed PIAs		
		http://www.management.energy.gov/FOIA/PrivacyImpactAssessments.htm		
U.S. Department of the Treasury (Treasury)	**Privacy Act Handbook**	**Privacy Policy and Legal Notices for U.S. Department of the Treasury Publicly Accessible Web Sites**	**U.S. Department of the Treasury Directive re: Certification Process for the Use of Persistent Cookies on Treasury Web Sites**	**U.S. Department of the Treasury Directive re: The Treasury Data Integrity Board**
	http://www.treas.gov/foia/reading-room/tdp25-04.pdf	http://www.treas.gov/privacy.htm	http://www.treas.gov/regs/td81-08.htm	http://www.treas.gov/regs/td25-06.htm
	Privacy Act Policies			
	http://www.treas.gov/foia/privacy/			
	Privacy Act Issuances http://www.treas.gov/foia/privacy/issuances/treasurypa.html			
	Privacy Act Exemption Regulations			
	http://www.treas.gov/foia/privacy/paregs.html			
	Treasury Directive re: The Privacy Act of 1974, as Amended			
	http://www.treas.gov/foia/reading-room/index.html			

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Department of the Interior (DOI)	Privacy Act System of Records Notices	Web Site Policy	Children's Privacy Policy	Protecting Sensitive Data When Transferring, Donating, or Disposing of Computer Equipment
	http://www.doi.gov/ocio/privacy/List_doipa_notices_9.03.htm	http://www.doi.gov/privacy.html	http://www.doi.gov/chprivacy.html	http://www.doi.gov/ocio/privacy/Disposing%20Sensitive%20Data%20CIO%20Memo%202001-004.htm
		Samples of Component Web Site Policies	Guidance on Interagency Sharing of Personal Data, and Privacy Protection Measures in System Development and Applications	Example Language for Addressing Records Management Compliance in Contracts
		http://www.usgs.gov/laws/privacy.html	http://www.doi.gov/ocio/privacy/Sharing%20of%20Sensitive%20Data_PIA%20CIO%20Memo%202001-002.htm	http://www.archives.gov/records-mgmt/toolkit/pdf/ID192.pdf
		http://www.nps.gov/privacy.htm		
		http://www.blm.gov/blm_info/privacy.htm		
		Privacy Impact Assessment Guidance		
		http://www.doi.gov/ocio/privacy/DOI%20PIA_03.01.04.doc		
		Safeguarding of Privacy Act Records		
		http://www.doi.gov/ocio/privacy/manual/383DM8.htm		
Executive Office of the President (EOP)				Memoranda Concerning Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security
				http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm
U.S. Postal Service (USPS)	Guide to Privacy and the Freedom of Information Act	Web Site Policy	Cookies and Web Analysis Tools on USPS.com	Postal Service Policy on Collection of Information From Children
	http://www.usps.com/cpim/ftp/hand/as353/welcome.htm	http://www.usps.com/common/docs/privpol.htm	http://www.usps.com/common/docs/pmg_cookie_letter.pdf	http://www.usps.com/common/docs/children.htm
	http://www.usps.com/privacyoffice/welcome.htm			
		Business/Privacy Impact Assessment Guidance		
		http://www.usps.com/privacyoffice/_pdf/AS805ABIA383.pdf		

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Office of Personnel Management (OPM)	OPM_Government-Wide_Privacy_Act_Systems https://www.opm.gov/feddata/html/privacy.asp		Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft http://www.dod.mil/pubs/foi/privacy/OPM_18June2007.pdf	
U.S. Securities and Exchange Commission (SEC)		Privacy Impact Assessment Guidance http://www.sec.gov/about/privacy/piaguide.pdf		
U.S. General Services Administration (GSA)	GSA Guide—Protecting Personally Identifiable Information http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/USA%20Services%20Newsletter%2005-07_R2-v-x9-c_0Z5RDZ-i34K-pR.pdf			
Federal Trade Commission (FTC)		Web Site Policy http://www.ftc.gov/ftc/privacy.shtm	DOI New Employee Orientation Page on Privacy http://www.doiu.nbc.gov/orientation/privacy_act.html	The Gramm-Leach-Bliley Act: The Financial Privacy Rule http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html
		Privacy Impact Assessments http://www.ftc.gov/ftc/privacyimpactassessment.shtm	DOI Privacy Training for IT Professionals http://www.doi.gov/ocio/privacy/Privacy%20for%20IT%20Professionals_10.16.05.ppt	
				The Children's Online Privacy Protection Act http://www.ftc.gov/privacy/privacyinitiatives/childrens.html
				Protecting Personal Information: A Guide for Business
				http://www.ftc.gov/infosecurity/
				Education and Guidance
				http://www.ftc.gov/privacy/privacyinitiatives/promises_educ.html

Federal Agency	Privacy Act Compliance Policies	E-Government Act Compliance Policies	Policies developed in response to OMB requirements	Miscellaneous
U.S. Office of Management and Budget (OMB)		Web Site Policy		Guidance on Interagency Sharing of Personal Data—Protecting Personal Privacy
		http://www.whitehouse.gov/privacy.html		http://www.whitehouse.gov/omb/memoranda/m01-05.html
				Safeguarding Against and Responding to the Breach of Personally Identifiable Information
				http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
				Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
				http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf
				Protection of Sensitive Agency Information
				http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf
				Safeguarding Personally Identifiable Information
				http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf

Page is intentionally left blank.

Appendix H
ISE Privacy Guidelines Definitions

Page is intentionally left blank.

ISE Privacy Guidelines Definitions

Information Sharing Environment (ISE)—The Information Sharing Environment (ISE) is an approach to the sharing of terrorism and homeland security information that is being implemented through a combination of policies, procedures, and technologies designed to facilitate access to critical information by all relevant entities. The ISE serves the dual imperatives of enhanced information sharing to combat terrorism and protecting the information privacy and other legal rights of Americans in the course of increased information access and collaboration across and among levels of government and elements of the private sector. The ISE is being developed pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (IRTPA, Section 1016) and Executive Order 13388, entitled "Further Strengthening the Sharing of Terrorism Information to Protect Americans."

IRTPA—"IRTPA" stands for the Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 108-458, as amended by Public Law 110-53. The ISE is covered by Section 1016 of IRTPA, codified at 6 USC 485.

ISE Privacy Official—The ISE Privacy Official is the official responsible for directly overseeing the agency's implementation of and compliance with the ISE Privacy Guidelines. The agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or executive order or as otherwise identified in response to the Office of Management and Budget (OMB) Memorandum M-05-08 dated February 11, 2005) will serve as the ISE Privacy Official, unless the head of the agency determines that a different official would be better situated to perform this role. See Section 12(a) of the ISE Privacy Guidelines.

ISE Privacy Guidelines Committee—The ISE Privacy Guidelines Committee is a standing committee established by the PM-ISE and is composed of each Information Sharing Council agency's ISE Privacy Official. The Committee provides ongoing guidance on the implementation of the ISE Privacy Guidelines, so that, among other things, agencies follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an interagency basis. See Section 12(b) of the ISE Privacy Guidelines.

PM-ISE—PM-ISE stands for the Program Manager for the Information Sharing Environment. This position was established by IRTPA Section 1016(f) and is further described within this document.

Protected Information—Protected Information is information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under the U.S. Constitution and federal laws of the United States. Protected information may also include other information that the U.S. government expressly determines (by Executive Order, international agreement, or other similar instrument) should be covered by these Guidelines. For the Intelligence Community, protected information includes information about United States persons as defined in Executive Order 12333, which provides that a U.S. person is "a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." (See Section 1 of the ISE Privacy Guidelines.) The definition of protected information may also include legal protections that are not strictly related to privacy. For example, information relating to the exercise of rights under the First Amendment may be subject to constitutional protections. And for the

Intelligence Community, information about U.S. corporations or associations that does not reveal personally identifiable information may nonetheless be subject to protection under Executive Order 12333. However, it is anticipated that in most cases, protections will focus on personally identifiable information about U.S. citizens and lawful permanent residents.

Terrorism Information—Terrorism Information is defined in IRTPA Section 1016 (codified at 6 USC 485) as all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:

- The existence, organization, capabilities, plans, intentions, vulnerabilities, means of financial or material support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism;
- Threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
- Communications of or by such groups or individuals; or
- Groups of individuals reasonably believed to be assisting or associated with such groups or individuals.

The definition includes weapons of mass destruction information.

Homeland Security Information—Homeland Security Information, as derived from the Homeland Security Act of 2002, Public Law 107-296, Section 892(f)(1) (codified at 6 USC 482(f)(1)) is defined as any information possessed by a state, local, tribal, or federal agency that:

- Relates to a threat of terrorist activity;
- Relates to the ability to prevent, interdict, or disrupt terrorist activity;
- Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
- Would improve the response to a terrorist act.

Law Enforcement Information—Law Enforcement Information is defined as any information obtained by or of interest to a law enforcement agency or official that is both:

- Related to terrorism or the security of our homeland, and
- Relevant to a law enforcement mission, including but not limited to:
    - Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation;
    - Assessment of or response to criminal threats and vulnerabilities;
    - The existence, organization, capabilities, plans, intention, vulnerabilities, means, method, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct;
    - The existence, identification, detection, prevention, interdiction, or disruption of, or response to criminal acts and violations of the law;
    - Identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and
    - Victim/witness assistance.

Weapons of Mass Destruction Information—Weapons of Mass Destruction Information is defined in IRTPA Section 1016 (codified at 6 USC 485) as information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical,

biological, radiological, or nuclear weapon) that could be used by a terrorist or terrorist organization against the United States, including information about the location of a stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or terrorist organization against the United States.

For more information and latest Workbook updates, go to

www.ise.gov/pages/privacy-implementing.html